Patent Application Laid-Open No. H 10-135945
Laid-Open Date: May 22, 1998
Patent Application No. H 8-291452
Application date: November 1, 1996
No Examination Requested
Applicant: K.K. Toshiba
Inventors: June Inoue et al
Title of the Invention:
Mobile Computer, Packet Processing Apparatus and Communication Controlling Method
Corresponding United States Patent Number 6.167,513

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－135945

(43)公開日　平成10年(1998)５月22日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32	---	Ｈ０４Ｌ	9/00	６７１
Ｇ０６Ｆ	13/00	３５５	Ｇ０６Ｆ	13/00	３５５
	15/00	３３０		15/00	３３０Ａ
Ｈ０４Ｌ	12/56		Ｈ０４Ｌ	11/20	１０２Ｚ

審査請求　未請求　請求項の数23　ＯＬ　（全 36 頁）

(21)出願番号　特願平8－291452

(22)出願日　平成８年(1996)11月１日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　井上　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　石山　政浩
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　福本　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(74)代理人　弁理士　鈴江　武彦　（外６名）

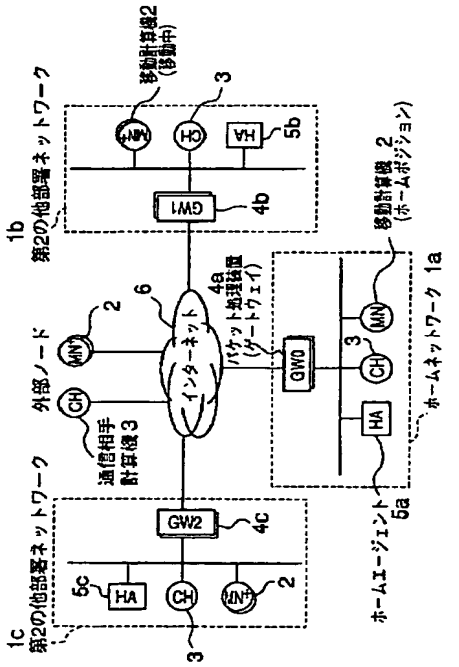
最終頁に続く

(54)【発明の名称】　移動計算機装置、パケット処理装置及び通信制御方法

(57)【要約】

【課題】　自装置の現在位置に応じて移動情報の登録、通信相手へのパケット転送を正しく行えるようにした移動計算機装置を提供すること。

【解決手段】　ホームネット内の計算機がネット外へ向けて送信するパケットを暗号化認証処理する機能を持つパケット処理装置が設置されたネットワークを含む複数のネットワークが相互接続された通信システム内を移動通信可能な移動計算機装置であって、自装置が、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する管理装置の設置されたホームネット内に位置するか否かを認識する手段と、自装置及び自装置が通信相手とする計算機の少なくとも一方につきその送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識する手段と、これら認識結果に基づき、送信すべきパケットの暗号化認証処理を含む所定の通信処理を行う手段とを具備する。



1

【特許請求の範囲】

【請求項１】ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置が設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内を移動して通信を行うことが可能な移動計算機装置であって、

自装置が、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークの内部に位置するか外に位置するかを認識する第１の認識手段と、

自装置及び自装置が通信相手とする計算機の少なくとも一方につき、その送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識する第２の認識手段と、

これら第１及び第２の認識手段の認識結果に基づき、送信すべきパケットの暗号化認証処理を含む所定の通信処理を行う手段とを具備することを特徴とする移動計算機装置。

【請求項２】前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識された場合、

該移動計算機管理装置へ向けて、所定の暗号化認証処理を施した、自装置の現在位置情報を含む登録メッセージを送信し、

これに対し経路途中のパケット処理装置から通過拒否応答が返信された場合、該パケット処理装置の認証用鍵情報を検索し、この認証用鍵を使った認証コードを登録メッセージに付加して再送信することを特徴とする請求項１に記載の移動計算機装置。

【請求項３】前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識された場合、

該ネットワークの内部の前記移動計算機管理装置へ向けて、現在位置情報を含む登録メッセージを、暗号化認証処理せずに送信することを特徴とする請求項１に記載の移動計算機装置。

【請求項４】前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識された場合、

自装置が通信相手とする計算機に向けて、暗号化認証処理せずにパケットを送信することを特徴とする請求項１に記載の移動計算機装置。

【請求項５】前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、そのパケット処理装置が一致すると認識された場合、

自装置が通信相手とする計算機に向けて、暗号化認証処理せずにパケットを送信することを特徴とする請求項１に記載の移動計算機装置。

2

【請求項６】前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とする他のパケット処理装置が存在すると認識され、さらに、既に該パケット処理装置が自装置の送信するパケットを認証処理なしに外部へ通過させるものであることが判明している場合、

自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データを付加されたパケットを送信することを特徴とする請求項１に記載の移動計算機装置。

【請求項７】前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とする他のパケット処理装置が存在すると認識され、さらに、既に該パケット処理装置が自装置の送信するパケットを認証処理なしには外部へ通過させないものであることが判明している場合、

自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データおよび経路間認証データの付加されたパケットを送信することを特徴とする請求項１に記載の移動計算機装置。

【請求項８】前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識された場合、

自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データの付加されたパケットを送信することを特徴とする請求項１に記載の移動計算機装置。

【請求項９】前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識され場合、

自装置が通信相手とする計算機に向けて、暗号化認証処理せずにパケットを送信することを特徴とする請求項１に記載の移動計算機装置。

【請求項１０】前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置

されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識された場合、

自装置が通信相手とする計算機との間で、暗号通信は行わず、かつ、自装置が移動先で獲得したアドレスを使用して通信相手となる計算機と直接通信することを特徴とする請求項１に記載の移動計算機装置。

【請求項１１】前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在せず、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識された場合、

自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークに対して所定の通信内容が暗号化されたパケットを送信し、該ネットワーク内のパケット転送装置によりアドレスを変換して自装置が通信相手とする計算機に転送してもらうとともに、

自装置が通信相手とする計算機から送信されるパケットは、該パケット転送装置によりアドレス変換した後に、移動計算機管理装置で経路制御し、所定の通信内容を暗号化して自装置に転送してもらうことを特徴とする請求項１に記載の移動計算機装置。

【請求項１２】ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内に設置され、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置であって、

転送すべきパケットの送信元となる計算機及び宛先となる計算機の少なくとも一方について、その計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機か否かを認識する第１の認識手段と、

前記計算機の少なくとも一方について、その計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識する第２の認識手段と、

これら第１及び第２の認識手段の認識結果に基づき、前記計算機間で通信されるパケットの暗号化認証処理を含む所定の通信処理を行う手段とを具備することを特徴とするパケット処理装置。

【請求項１３】前記第２の認識手段により、自装置が該

移動計算機が送信するパケットを暗号化認証処理対象とすることが認識された場合、

前記移動計算機から、自装置宛の経路認証データの付加されていないパケットを受信したならば、通過拒否メッセージを前記移動計算機に返信し、

前記移動計算機から、自装置宛の経路間認証データの付加されたパケットを受信したならば、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを次段ノードに対する経路間認証データに換えて転送し、

前記計算機宛の応答メッセージを受信したならば、自装置宛の経路間認証データを検査し、該経路間認証データの正当性が確認されたならば、該経路間認証データを除いて前記移動計算機に転送し、

自装置が前記移動計算機管理装置の設置されたネットワークに位置する場合、

前記移動計算機管理装置からの応答メッセージを受信したならば、所定の通信内容を暗号化しかつ末端認証データ及び次段ノードに対する経路間認証データを付加して該応答メッセージを前記移動計算機に宛てて転送することを特徴とする請求項１２に記載のパケット処理装置。

【請求項１４】前記第１の認識手段により、いずれの計算機も、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機ではないと認識され、かつ、前記第１の認識手段により、いずれの計算機についても、その計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、

暗号化されていないパケットが転送されて来たとき、所定の通信内容を暗号化しかつ末端認証データを付加して転送し、所定の通信内容が暗号化されかつ末端認証データを付加されたパケットが転送されて来たとき、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号してパケットを転送することを特徴とする請求項１２に記載のパケット処理装置。

【請求項１５】前記第１の認識手段により、少なくとも一方の計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であると認識され、前記第２の認識手段により、該一方の計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識され、かつ、前記第１の認識手段及び前記第２の認識手段により、他方の計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機ではなくかつその送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないもの、ではないと認識された場合、

少なくとも転送すべき入力パケットのパケット形式に基づき、前記計算機間で通信されるパケットの暗号化認証

処理を含む所定の通信処理を行うことを特徴とする請求項１２に記載のパケット処理装置。

【請求項１６】暗号化されていないデータパケットが転送されて来た場合、所定の通信内容を暗号化しかつ末端認証データを付加して転送し、所定の通信内容が暗号化されかつ末端認証データを付加されたパケットが転送されて来た場合、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号してパケットを転送することを特徴とする請求項１５に記載のパケット処理装置。

【請求項１７】自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であって、自装置が暗号化認証処理対象とするものを送信元とする、所定の通信内容が暗号化されかつ末端認証データを付加されたパケットが転送されて来た場合、次段ノードに対する経路間認証データを付加して転送し、

前記移動計算機を送信元とする、所定の通信内容が暗号化されかつ末端認証データ及び自装置に対する経路間認証データを付加されたパケットが転送されて来た場合、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを次段ノードに対する経路間認証データに換えて転送することを特徴とする請求項１５に記載のパケット処理装置。

【請求項１８】自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であって、自装置が暗号化認証処理対象とするものを宛先とする、所定の通信内容が暗号化されかつ末端認証データ及び自装置に対する経路間認証データを付加されたパケットが転送されて来た場合、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送することを特徴とする請求項１５に記載のパケット処理装置。

【請求項１９】自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機でない計算機であって、自装置が暗号化認証処理対象とするものを宛先とする、所定の通信内容が暗号化されかつ自装置に対する末端認証データ及び経路間認証データを付加されたパケットが転送されて来た場合、該末端認証データ及び該経路間認証データを夫々検査し、該末端認証データ及び該経路間認証データの正当性がいずれも認識されたならば、該末端認証データ及び該経路間認証データを取り除き所定の通信内容を復号して転送することを特徴とする請求項１５に記載のパケット処理装置。

【請求項２０】自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機を宛先とし、他の計算機を送信元とするパケットであって、該移動計算機管理装置により中継されたことが示されるパケットが転送されてきた場合、該移動計算機を暗号化認証処理対象とするパケット処理装置が存在すると認識されたならば、所定の通信内容を暗号化しかつ該移動計算機に対する末端認証データ及び次段ノードに対する経路間認証データを付加してパケットを転送し、該移動計算機を暗号化認証処理対象とするパケット処理装置が存在しないと認識されたならば、所定の通信内容を暗号化しかつ該移動計算機に対する末端認証データを付加してパケットを転送することを特徴とする請求項１５に記載のパケット処理装置。

【請求項２１】経路最適化を要求された際に、前記第１及び第２の認識手段による認識結果に基づいて自装置が経路最適化に寄与するものであると認識された場合、前記認識結果に応じた所定の経路最適化処理を行うことを特徴とする請求項１２、１５、１６または１７に記載のパケット処理装置。

【請求項２２】ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置が設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内を移動して通信を行うことが可能な移動計算機装置の通信制御方法であって、

自装置が、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークの内部に位置するか外に位置するかを認識するとともに、

自装置及び自装置が通信相手とする計算機の少なくとも一方につき、その送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識し、

これら認識結果に基づき、送信すべきパケットの暗号化認証処理を含む所定の通信処理を行うことを特徴とする通信制御方法。

【請求項２３】ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内に設置され、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置の通信制御方法であって、

転送すべきパケットの送信元となる計算機及び宛先となる計算機の少なくとも一方について、その計算機が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機か否かを認識し、

前記計算機の少なくとも一方について、その計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識し、

これら認識結果に基づき、前記計算機間で通信されるパ

ケットの暗号化認証処理を含む所定の通信処理を行うことを特徴とする通信制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、移動計算機装置、パケット処理装置及び通信制御方法に関する。

【０００２】

【従来の技術】計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみならず、オフィス外、１組織外とのコミュニケーション（電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（Ｉｎｔｅｒｎｅｔ）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。

【０００３】また、このようなネットワークの普及に伴い、移動通信（ｍｏｂｉｌｅ　ｃｏｍｐｕｔｉｎｇ）に対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持ったユーザがネットワーク上を移動して通信する。ときには通信を行いながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上のアドレスを管理し、正しく通信内容を到達させるための方式が必要である。

【０００４】また、ネットワークが普及し、ネット間の自由な接続が実現され、膨大なデータ、サービスのやりとりがなされる場合、セキュリティ上の問題を考慮する必要が生じてくる。例えば、組織内部の秘密情報の外部ネットワークへの漏洩をいかに防ぐか、という問題や、組織外からの不正な侵入から、組織内ネットワークに接続された資源、情報をいかに守るか、という問題である。インターネットは、当初学術研究を目的に構築されたため、ネットワークの接続による自由なデータサービスのやりとりを重視しており、このようなセキュリティ上の問題は考慮されていなかったが、近年多くの企業、団体がインターネットに接続するようになり、セキュリティ上の問題から自組織ネットワークを防衛する機構が必要となってきた。

【０００５】そこで、インターネット上でデータパケットを交換する際に、外部にデータパケットを送出する前にその内容を暗号化し認証コードをつけ、受信したサイトで認証コードを確認し復号化する、という方法がある。例えば、インターネットの標準化団体であるＩＥＴＦにおいては、ＩＰパケットの暗号化、認証コード付与方式をＩＰセキュリティ標準（文献：ＩＥＴＦ　ＲＦＣ１８２５～１８２９）として規定している。この方法によれば、たとえ組織外のユーザが外部ネットワーク上のデータパケットを取り出しても、内容が暗号化されているので、決してその内容が漏洩することがなく、安全な通信が確保できる。

【０００６】このような暗号化通信をサポートするゲートウェイ計算機で守られた（ガードされた）ネットワーク同士であれば相互に暗号化通信が可能であり、また前述の移動計算機が自分でパケットの暗号化、復号を行う機能をサポートしていれば、任意のゲートウェイ間、またはゲートウェイ～移動計算機間で暗号化通信がサポートできる。例えば、図４２では、元々ホームネットワーク１ａに属していた移動計算機２が、他のネットワーク１ｂに移動し、ネットワーク１ｃ内の他の計算機３（ＣＨ）と暗号化、復号機能をサポートするゲートウェイ４ａ，４ｃを介して暗号通信を行う。

【０００７】一般に移動通信を行う場合、移動計算機の移動先データを管理するルータ（ホームエージェント）を置き、移動計算機宛データの送信はそのホームエージェントを経由して、移動計算機のもとのアドレス宛のＩＰパケットを移動ＩＰの現在位置アドレス宛パケット内にカプセル化することで移動計算機に対するデータの経路制御を行う。図４２では、ホームエージェント５（ＨＡ）がこの役割を行う。

【０００８】この方式は、やはりＩＥＴＦのｍｏｂｉｌｅ－ＩＰワーキンググループで標準化が進められている移動ＩＰと呼ばれる方式である（文献：ＩＥＴＦ　ＲＦＣ２００３－２００６）。

【０００９】この移動ＩＰ方式と、先のＩＰセキュリティによるデータパケットの暗号化を組み合わせて使用すると、図４２におけるパケットの転送経路は、ＣＨ→ゲートウェイ４ｃ（暗号化）→ゲートウェイ４ａ（復号）→ＨＡ→ゲートウェイ４ａ（暗号化）→移動計算機２（復号）となる。

【００１０】このように移動ＩＰおよびＩＰセキュリティによるパケット暗号化を併用する場合、移動計算機およびその通信相手の現在位置の各場合に応じて、各構成要素の動作を変更するよう制御することが必要になる。

【００１１】例えば、システムが、図１に示すような構成であるとする。ここで、ＭＮは移動計算機、ＣＨはその通信相手を示している。ＧＷはパケット暗号化装置、ＨＡはホームエージェントを示す。また、MN^+ はＧＷ（パケット暗号化認証処理）機能を自分でサポートする移動計算機である。移動計算機ＭＮのホームドメインネットワークのことを「ホームネット」と呼ぶ。また、

「ＧＷ保護域内」とは、ゲートウェイで保護されたネットワークを指し、「ＧＷ保護域外」とは、それ以外の外部を指す。

【００１２】まず、図１７に示すように、ＭＮとＣＨのそれぞれがＧＷ保護域の内部か外部かで［１］～［４］の４つケースに大分類される。

【００１３】なお、ここでは、ＣＨは、固定計算機で暗号化認証処理を行わないものと仮定している。

【００１４】さらに、上記の［１］［２］のＧＷを介した通信のケースを細分類すると、図１８に示すように、（１）～（７）の７つのケースに分類される。

【００１５】各々のケースについて、各ノードの処理、各ＧＷでのＩＰセキュリティ処理が異なってくるので、移動ＩＰ、ＩＰセキュリティの併用の際には、移動計算機、通信相手の位置情報をもとに、上記の［１］、［２］、（１）～（７）ケースの分類を行うことが重要になる。

【００１６】また、通信相手の位置によっては、パケット暗号化を使用できない場合もある。例えば、通信相手がまったくパケット暗号化装置のない、ネットワークにいる場合である。これは、上記の［３］［４］の場合に相当する。このような場合は、移動計算機は、移動プロトコルのみを使用することになる。

【００１７】また、移動ＩＰでは、ホームエージェント経由の移動計算機宛のパケット経路を、各ネットワーク構成要素が正しい位置情報をキャッシュして保持している場合に最適化することを規定している。この経路最適化も、パケット暗号化を併用する場合、移動計算機と通信相手の現在位置を認識して、適用可能性を判定することが必要になる。

【００１８】例えば、上記の（５）のケース（通信相手ＣＨと移動計算機ＭＮが別の部署に位置するケース）であると認識できれば、図４３に示すような経路最適化が可能である。

【００１９】また、移動ＩＰ方式では、移動計算機が新規の移動先に移った場合、現在位置の登録メッセージをホームエージェントに送ることが必要である。この場合も、移動計算機がホームネットワークと親しいネットワークに移動して、そのゲートウェイが登録メッセージを自由に外部に送出させる場合は、移動ＩＰの規定のままで動作が可能だが、一般に移動計算機を外部から内部に滞在しているものとして扱うネットワークでは、セキュリティ上の考慮から、移動計算機の発するメッセージを自由に外部に送出させることは危険である。この場合、移動計算機が、自分は現在自分を侵入者として扱うネットワークにいる、ということを認識し、ゲートウェイに対して身分証明に相当する処理を行って外部アクセス許可を得た後に登録メッセージのあとの実際のデータ転送においても、ゲートウェイに対する身分証明を保持しての通信が必要である。

【００２０】

【発明が解決しようとする課題】従来は、移動ＩＰ方式では、各ネットワークノードは一意なＩＰアドレスが付与され、自由に制御パケットをやりとりできるという仮定で、経路制御や移動計算機位置の登録などの規定を行っていたため、実際の運用に際しては、移動計算機がどのような組織に属するネットワークに移動したか、というネットワーク運用ポリシーに関する動作規定がなく、移動ＩＰおよびＩＰセキュリティによるパケット暗号化を併用する場合、移動計算機およびその通信相手の現在位置の各ケースに応じ、各移動計算機とＩＰパケット暗号化を行うパケット暗号化装置の動作を変更するように制御することができなかった。また、移動ＩＰの経路最適化も困難であった。

【００２１】また、移動ＩＰの規定はネットワーク運用ポリシーを考慮していないため、例えば外部組織のネットワークに移動して移動ＩＰの登録メッセージをホームネットワーク宛に送信する場合、外部ネットワークのゲートウェイが外向きパケットをすべて許すのであれば、移動ＩＰの規定がそのまま使用できるが、一般にこれがセキュリティの観点から望ましくない。このため特にセキュリティを考慮し内部計算機の自由な外部アクセスを許可しないようなネットワークに移動計算機が移動した場合、移動後に行う新規位置の登録メッセージさえも移動計算機のホームネットワーク上のホームエージェントに到達させることができず、移動計算機に関する運用に障害を起こすことがあった。

【００２２】本発明は、上記事情を考慮してなされたもので、相互に接続されたネットワーク間を移動して暗号通信を行うことが可能な移動計算機において、ネットワーク運用ポリシーを考慮し自装置の現在位置に応じた適正なパケット転送を行うことの可能なパケット処理装置及び通信制御方法を提供することを目的とする。

【００２３】また、本発明は、上記事情を考慮してなされたもので、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機をサポートするとともに暗号通信をサポートする通信ネットワークにおいて、ネットワーク運用ポリシーを考慮しパケット通信する計算機の現在位置に応じた適正なパケット転送を行うことの可能なパケット処理装置及び通信制御方法を提供することを目的とする。

【００２４】

【課題を解決するための手段】本発明（請求項１）は、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置（例えば、パケット暗号化認証処理機能を持つゲートウェイ）が設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内を移動して通信を行うことが可能な移動計算機装置であって、自装置が、自装置の移動位置情報を管理

し自装置宛のパケットを自装置の現在位置に転送する手段を有する移動計算機管理装置（例えば、ホームエージェント）の設置されたネットワークの内部に位置するか外に位置するかを認識する第１の認識手段と、自装置及び自装置が通信相手とする計算機の少なくとも一方につき、その送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識する第２の認識手段と、これら第１及び第２の認識手段の認識結果に基づき、送信すべきパケットの暗号化認証処理を含む所定の通信処理を行う手段とを具備することを特徴とする。

【００２５】暗号化認証処理を含む所定の通信処理には、例えば、パケットを暗号化せずに送信する処理、パケットの所定の通信情報を暗号化しかつ暗号通信に係る末端ノード間で行う認証のための末端認証データを付加してパケットを送信する処理、パケットの所定の通信情報を暗号化しかつ暗号通信に係る末端ノード間で行う認証のための末端認証データおよび次段のパケット処理装置との間で行う認証のための経路間認証データを付加してパケットを送信する処理が含まれる。

【００２６】より具体的には、例えば、移動ＩＰにおける、通常のＩＰ形式のパケットを送信する処理、暗号化／末端認証形式のパケットを送信する処理、暗号化／経路間認証形式のパケットを送信する処理が含まれる。

【００２７】また、移動計算機は、受信したパケットが暗号化され末端認証データが付加されている場合には、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して実際の転送データを得る。

【００２８】本発明（請求項２）は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識された場合、該移動計算機管理装置へ向けて、所定の暗号化認証処理を施した、自装置の現在位置情報を含む登録メッセージを送信し、これに対し経路途中のパケット処理装置から通過拒否応答が返信された場合、該パケット処理装置の認証用鍵情報を検索し、この認証用鍵を使った認証コードを登録メッセージに付加して再送信することを特徴とする。

【００２９】本発明（請求項３）は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識された場合、該ネットワークの内部の前記移動計算機管理装置へ向けて、現在位置情報を含む登録メッセージを、暗号化認証処理せずに送信することを特徴とする。

【００３０】本発明（請求項４）は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識された場合、自装置が通信相手とする計算機に向けて、暗号化認証処理せずにパケット（例えば、通常のＩＰ形式のパケット）を送信することを特徴とする。

【００３１】本発明（請求項５）は、請求項１に記載の移動計算機装置において、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、そのパケット処理装置が一致すると認識された場合、自装置が通信相手とする計算機に向けて、暗号化認証処理せずにパケット（例えば、通常のＩＰ形式のパケット）を送信することを特徴とする。

【００３２】本発明（請求項６）は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とする他のパケット処理装置が存在すると認識され、さらに、既に該パケット処理装置が自装置の送信するパケットを認証処理なしに外部へ通過させるものであることが判明している場合、自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データを付加されたパケット（例えば、暗号化／末端認証形式パケット）を送信することを特徴とする。

【００３３】本発明（請求項７）は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とする他のパケット処理装置が存在すると認識され、さらに、既に該パケット処理装置が自装置の送信するパケットを認証処理なしには外部へ通過させないものであることが判明している場合、自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データおよび経路間認証データの付加されたパケット（例えば、暗号化／経路間認証形式パケット）を送信することを特徴とする。

【００３４】本発明（請求項８）は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装

置が存在しないと認識された場合、自装置が通信相手とする計算機に向けて、所定の通信内容が暗号化されかつ末端認証データの付加されたパケット（例えば、暗号化／末端認証形式パケット）を送信することを特徴とする。

【００３５】本発明（請求項９）は、請求項１に記載の移動計算機装置において、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識され場合、自装置が通信相手とする計算機に向けて、暗号化認証処理せずにパケット（例えば、通常のＩＰ形式のパケット）を送信することを特徴とする。

【００３６】また、本発明は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識され、かつ、前記第２の認識手段により、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識された場合、自装置が通信相手とする計算機との間で、暗号通信は行わず、かつ、直接通信をすることを特徴とするようにしても良い。

【００３７】また、本発明は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識された場合、自装置が通信相手とする計算機との間で、暗号通信は行わず、かつ、自装置宛のパケットは前記移動計算機管理装置で経路制御される通信を行うことを特徴とするようにしても良い。

【００３８】本発明（請求項１０）は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識された場合、自装置が通信相手とする計算機との間で、暗号通信は行わず、かつ、自装置が移動先で獲得したアドレスを使用して通信相手となる計算機と直接通信することを特徴とする。

【００３９】本発明（請求項１１）は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在せず、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないと認識された場合、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークに対して所定の通信内容が暗号化されたパケットを送信し、該ネットワーク内のパケット転送装置（例えば、プロシキー・サーバ）によりアドレスを変換して自装置が通信相手とする計算機に転送してもらうとともに、自装置が通信相手とする計算機から送信されるパケットは、該パケット転送装置によりアドレス変換した後に、移動計算機管理装置で経路制御し、所定の通信内容を暗号化して自装置に転送してもらうことを特徴とする。

【００４０】また、本発明は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識され、かつ、前記第２の認識手段により、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、該パケット処理装置が自装置を処理対象とするパケット処理装置と一致しないと認識された場合、自計算機を暗号化認証処理対象とするパケット処理装置にパケットを送信して自装置が通信相手とする計算機と暗号化通信を行い、通信相手も移動計算機宛に直接暗号化パケットを送信することを特徴とするようにしても良い。

【００４１】また、本発明は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、そのパケット処理装置が一致すると認識された場合（自装置の送信するパケット及び自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とする同一のパケット処理装置が存在すると認識された場合）、自装置が通信相手とする計算機に対し、暗号化認証処理せずにデータパケットを直接送信することを特徴とするようにしても良い。

【００４２】また、本発明は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケ

ットを暗号化認証処理対象とするパケット処理装置が存在せず、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、自装置が通信相手とする計算機に対し、暗号化されかつ認証データを付与されたパケットを送信することを特徴とするようにしても良い。

【００４３】また、本発明は、請求項１に記載の移動計算機装置において、前記第１の認識手段により、自装置が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、前記第２の認識手段により、自装置の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、自装置が通信相手とする計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在し、それらパケット処理装置が一致しないと認識された場合（自装置の送信するパケット及び自装置が通信相手とする計算機の送信するパケットを夫々暗号化認証処理対象とする同一でないパケット処理装置が存在すると認識された場合）、自装置が通信相手とする計算機に対し、通信内容が暗号化され終端間の認証データおよび自装置の移動先ネットワークに置かれたパケット処理装置との認証データを付与されたパケットを送信することを特徴とするようにしても良い。

【００４４】本発明（請求項１２）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有する移動計算機管理装置（例えば、ホームエージェント）の設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内に設置され、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置（例えば、暗号化認証処理機能を持つゲートウェイ）であって、転送すべきパケットの送信元となる計算機及び宛先となる計算機の少なくとも一方について、その計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機か否か（後者の場合、固定計算機またはホームネットにいる移動計算機が該当する）を認識する第１の認識手段と、前記計算機の少なくとも一方について、その計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識する第２の認識手段と、これら第１及び第２の認識手段の認識結果に基づき、前記計算機間で通信されるパケットの暗号化認証処理を含む所定の通信処理を行う手段とを具備することを特徴とする。

【００４５】暗号化認証処理を含む所定の通信処理には、例えば、（ａ）通常の暗号化されていないパケット、（ｂ）移動計算機管理部で経路制御され暗号化されていないパケット、（ｃ）所定の通信情報が暗号化されかつ暗号通信に係る末端ノード間で行う認証のための末端認証データを付加されたパケット、（ｄ）パケットの所定の通信情報が暗号化されかつ暗号通信に係る末端ノード間で行う認証のための末端認証データおよび次段のパケット処理装置との間で行う認証のための経路間認証データを付加されたパケット、のいずれかを入力し、前記認識結果に基づいて、入力パケットを、同一のパケット形式であるいは他のパケット形式に変換して送信する処理が含まれる。

【００４６】なお、上記の（ａ）～（ｄ）の各々のパケット形式は、例えば、移動ＩＰにおける、通常のＩＰ形式、移動ＩＰ形式、暗号化／末端認証形式、暗号化／経路間認証形式である。

【００４７】また、パケット処理装置は、前記認識結果に基づいて、経路最適化の可能性を判定するとともに、自装置が経路最適化に寄与するものと認識された場合、前記認識結果に応じた経路最適化のための制御を行うことができる。

【００４８】本発明（請求項１３）は、請求項１２に記載のパケット処理装置において、前記第２の認識手段により、自装置が該移動計算機が送信するパケットを暗号化認証処理対象とすることが認識された場合、前記移動計算機から、自装置宛の経路認証データの付加されていないパケットを受信したならば、通過拒否メッセージを前記移動計算機に返信し、前記移動計算機から、自装置宛の経路間認証データの付加されたパケットを受信したならば、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを次段ノードに対する経路間認証データに換えて転送し、前記計算機宛の応答メッセージを受信したならば、自装置宛の経路間認証データを検査し、該経路間認証データの正当性が確認されたならば、該経路間認証データを除いて前記移動計算機に転送し、自装置が前記移動計算機管理装置の設置されたネットワークに位置する場合、前記移動計算機管理装置からの応答メッセージを受信したならば、所定の通信内容を暗号化しかつ末端認証データ及び次段ノードに対する経路間認証データを付加して該応答メッセージを前記移動計算機に宛てて転送することを特徴とする。

【００４９】本発明（請求項１４）は、請求項１２に記載のパケット処理装置において、前記第１の認識手段により、いずれの計算機も、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機ではないと認識され、かつ、前記第１の認識手段により、いずれの計算機についても、その計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、暗号化されていないパケットが転送されて来たとき、所定の通信内容を暗号化しかつ末端認証データを付加して転送し、所定の通信内容が暗号化されかつ末端認証データを

付加されたパケットが転送されて来たとき、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号してパケットを転送することを特徴とする。

【００５０】本発明（請求項１５）は、請求項１２に記載のパケット処理装置において、前記第１の認識手段により、少なくとも一方の計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であると認識され、前記第２の認識手段により、該一方の計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識され、かつ、前記第１の認識手段及び前記第２の認識手段により、他方の計算機が、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機ではなくかつその送信するパケットを暗号化認証処理対象とするパケット処理装置が存在しないもの、ではないと認識された場合、少なくとも転送すべき入力パケットのパケット形式に基づき、前記計算機間で通信されるパケットの暗号化認証処理を含む所定の通信処理を行うことを特徴とする。

【００５１】本発明（請求項１６）は、請求項１５に記載のパケット処理装置において、暗号化されていないデータパケットが転送されて来た場合、所定の通信内容を暗号化しかつ末端認証データを付加して転送し、所定の通信内容が暗号化されかつ末端認証データを付加されたパケットが転送されて来た場合、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号してパケットを転送することを特徴とする。

【００５２】本発明（請求項１７）は、請求項１５に記載のパケット処理装置において、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であって、自装置が暗号化認証処理対象とするものを送信元とする、所定の通信内容が暗号化されかつ末端認証データを付加されたパケットが転送されて来た場合、次段ノードに対する経路間認証データを付加して転送し、前記移動計算機を送信元とする、所定の通信内容が暗号化されかつ末端認証データ及び自装置に対する経路間認証データを付加されたパケットが転送されて来た場合、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを次段ノードに対する経路間認証データに換えて転送することを特徴とする。

【００５３】本発明（請求項１８）は、請求項１５に記載のパケット処理装置において、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機であって、自装置が暗号化認証処理対象とするものを宛先とする、所定の通信内容が暗号化されかつ末端認証データ及び自装置に対する経路間認証データを付加されたパケットが転送されて来た場合、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送することを特徴とする。

【００５４】本発明（請求項１９）は、請求項１５に記載のパケット処理装置において、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機でない計算機であって、自装置が暗号化認証処理対象とするものを宛先とする、所定の通信内容が暗号化されかつ自装置に対する末端認証データ及び経路間認証データを付加されたパケットが転送されて来た場合、該末端認証データ及び該経路間認証データを夫々検査し、該末端認証データ及び該経路間認証データの正当性がいずれも認識されたならば、該末端認証データ及び該経路間認証データを取り除き所定の通信内容を復号して転送することを特徴とする。

【００５５】本発明（請求項２０）は、請求項１５に記載のパケット処理装置において、自計算機を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機を宛先とし、他の計算機を送信元とするパケットであって、該移動計算機管理装置により中継されたことが示されるパケットが転送されてきた場合、該移動計算機を暗号化認証処理対象とするパケット処理装置が存在すると認識されたならば、所定の通信内容を暗号化しかつ該移動計算機に対する末端認証データ及び次段ノードに対する経路間認証データを付加してパケットを転送し、該移動計算機を暗号化認証処理対象とするパケット処理装置が存在しないと認識されたならば、所定の通信内容を暗号化しかつ該移動計算機に対する末端認証データを付加してパケットを転送することを特徴とする。

【００５６】本発明（請求項２１）は、請求項１２、１５、１６または１７に記載のパケット処理装置において、経路最適化を要求された際に、前記第１及び第２の認識手段による認識結果に基づいて自装置が経路最適化に寄与するものであると認識された場合、前記認識結果に応じた所定の経路最適化処理を行うことを特徴とする。

【００５７】また、本発明は、請求項１２に記載のパケット処理装置において、前記第１及び第２の認識手段により、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識され、かつ、移動計算機及び移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、前段で移動計算機が送信した、所定の通信内容が暗号化されかつ末端認証データ及び前段との経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認

証データを次段に対するものに換えて転送し、次段が移動計算機である、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送し、それ以外の、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該末端認証データ及び該経路間認証データを夫々検査し、該末端認証データ及び該経路間認証データの正当性がいずれも認識されたならば、該末端認証データ及び該経路間認証データを取り除き所定の通信内容を復号して転送し、移動計算機管理部で経路制御され、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データ及び次段に対する経路間認証データを付与して転送することを特徴とするようにしても良い。

【００５８】また、本発明は、請求項１２に記載のパケット処理装置において、前記第１及び第２の認識手段により、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが該移動計算機と同じネットワークに位置すると認識され、かつ、移動計算機及び移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送し、所定の通信内容が暗号化されかつ末端認証データが付与されたパケットを受信したら、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して転送し、移動計算機管理部で経路制御され、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データ及び次段に対する経路間認証データを付与して転送し、次段が移動計算機である、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送することを特徴とするようにしても良い。

【００５９】また、本発明は、請求項１２に記載のパケット処理装置において、前記第１及び第２の認識手段により、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが該移動計算機と同じネットワークに位置すると認識され、かつ、移動計算機及び移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、移動計算機に対するデータ転送経路の最適化が要求され、前記第２の認識手段により、自装置が通信相手計算機が送信するパケットを暗号化認証処理対象とすることが認識されたとき、通信相手計算機からの暗号化されていないパケットを受信したら、該パケットを移動計算機管理装置で経路制御されたものと同じ形式のパケットに変換して移動計算機に転送することを特徴とするようにしても良い。

【００６０】また、本発明は、請求項１２に記載のパケット処理装置において、前記第１及び第２の認識手段により、移動計算機が前記移動計算機管理装置の設置された第１のネットワークの外に位置し、移動計算機が通信相手とする固定ノードが該移動計算機と異なるネットワークでかつ第１のネットワークでないネットワークに位置すると認識され、かつ、前記第２の認識手段により、移動計算機及び移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送し、所定の通信内容が暗号化されかつ末端認証データが付与されたパケットを受信したら、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して転送し、前段で移動計算機が送信した、所定の通信内容が暗号化されかつ末端認証データ及び前段との経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを次段に対するものに換えて転送し、次段が移動計算機である、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送し、それ以外の、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該末端認証データ及び該経路間認証データを夫々検査し、該末端認証データ及び該経路間認証データの正当性がいずれも認識されたならば、該末端認証データ及び該経路間認証データを取り除き所定の通信内容を復号して転送し、移動計算機管理部で経路制御され、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データ及び次段に対する経路間認証データを付与して転送することを特徴とするようにしても良い。

【００６１】また、本発明は、請求項１２に記載のパケット処理装置において、前記第１及び第２の認識手段により、移動計算機が前記移動計算機管理装置の設置された第１のネットワークの外に位置し、移動計算機が通信相手とする固定ノードが該移動計算機と異なるネットワークでかつ第１のネットワークでないネットワークに位置すると認識され、かつ、前記第２の認識手段により、

移動計算機及び移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合であって、かつ、移動計算機に対するデータ転送経路の最適化が要求された場合、前記第２の認識手段により、自装置が移動計算機が送信するパケットを暗号化認証処理対象とすることが認識されたとき、前段で移動計算機が送信した、所定の通信内容が暗号化されかつ末端認証データ及び前段との経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを次段に対するものに換えて転送し、次段が移動計算機である、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該経路間認証データを検査し、該経路間認証データの正当性が認識されたならば、該経路間認証データを取り除いて転送し、前記第２の認識手段により、自装置が通信相手計算機が送信するパケットを暗号化認証処理対象とすることが認識されたとき、次段が通信相手計算機である、所定の通信内容が暗号化されかつ末端認証データ及び経路認証データを付与されたパケットを受信したら、該末端認証データ及び該経路間認証データを夫々検査し、該末端認証データ及び該経路間認証データの正当性がいずれも認識されたならば、該末端認証データ及び該経路間認証データを取り除き所定の通信内容を復号して転送し、前段で通信相手計算機が送信した、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データ及び経路間認証データを付与して移動計算機に転送することを特徴とするようにしても良い。

【００６２】また、本発明は、請求項１２に記載のパケット処理装置において、前記第１及び第２の認識手段により、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが前記移動計算機管理装置の設置されたネットワークの内部に位置すると認識され、かつ、移動計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在せず、移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、所定の通信内容が暗号化されかつ末端認証データを付与されたパケットを受信したら、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して転送し、移動計算機管理部で経路制御され、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送することを特徴とするようにしても良い。

【００６３】また、本発明は、請求項１２に記載のパケット処理装置において、前記第１及び第２の認識手段により、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、移動計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在せず、移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送し、所定の通信内容が暗号化されかつ末端認証データが付与されたパケットを受信したら、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して転送し、移動計算機管理部で経路制御され、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送することを特徴とするようにしても良い。

【００６４】また、本発明は、請求項１２に記載のパケット処理装置において、前記第１及び第２の認識手段により、移動計算機が前記移動計算機管理装置の設置されたネットワークの外に位置し、移動計算機が通信相手とする固定ノードが前記移動計算機管理装置の設置されたネットワークの外に位置すると認識され、かつ、移動計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在せず、移動計算機が通信相手とする固定ノードの送信するパケットを暗号化認証処理対象とするパケット処理装置が存在すると認識された場合であって、かつ、移動計算機に対するデータ転送経路の最適化が要求された場合、前記第２の認識手段により、自装置が通信相手計算機が送信するパケットを暗号化認証処理対象とすることが認識されたとき、暗号化されていないパケットを受信したら、所定の通信内容を暗号化しかつ末端認証データを付与して転送し、前段で通信相手計算機が送信した、所定の通信内容が暗号化されかつ末端認証データが付与されたパケットを受信したら、該末端認証データを検査し、該末端認証データの正当性が認識されたならば、該末端認証データを取り除き所定の通信内容を復号して転送して移動計算機に転送することを特徴とするようにしても良い。

【００６５】本発明（請求項２２）は、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置が設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内を移動して通信を行うことが可能な移動計算機装置の通信制御方法であって、自装置が、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークの内部に位置するか外に位置するかを認識するとともに、自

装置及び自装置が通信相手とする計算機の少なくとも一方につき、その送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識し、これら認識結果に基づき、送信すべきパケットの暗号化認証処理を含む所定の通信処理を行うことを特徴とする。

【００６６】本発明（請求項２３）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し該移動計算機宛のパケットを該移動計算機の現在位置に転送する手段を有する移動計算機管理装置の設置されたネットワークを含む複数のネットワークが相互に接続された通信システム内に設置され、ネットワーク内部の計算機が該ネットワーク外の計算機へ向けて送信するパケットを暗号化認証処理する手段を有するパケット処理装置の通信制御方法であって、転送すべきパケットの送信元となる計算機及び宛先となる計算機の少なくとも一方について、その計算機が、自装置を処理対象とする前記移動計算機管理装置の設置されたネットワークの外に移動中の移動計算機か否か（固定ノードまたはホームネットにいる移動計算機）を認識し、前記計算機の少なくとも一方について、その計算機の送信するパケットを暗号化認証処理対象とするパケット処理装置が存在するか否かを認識し、これら認識結果に基づき、前記計算機間で通信されるパケットの暗号化認証処理を含む所定の通信処理を行うことを特徴とする。

【００６７】従来、移動ＩＰ方式では、各ネットワークノードは一意なＩＰアドレスが付与され、自由に制御パケットをやりとりできるという仮定でのみ、経路制御や移動計算機位置の登録などの規定を行っていたが、本発明によれば、実際の運用に再して、移動計算機がどのような組織に属するネットワークに移動したか、というネットワーク運用ポリシーに関する動作規定、例えば暗号通信するか否か、認証を必要とするか否かなどを考慮することができる。

【００６８】また、ＩＰセキュリティにもとづく暗号化装置を介して暗号化、認証通信を行う場合、各移動計算機およびその通信相手の位置に応じて各ネットワーク構成要素の動作が大きく変化する。特に、暗号化認証処理をともなって、移動ＩＰの経路最適化を行うためにも、この位置情報認識を有効に利用できる。

【００６９】また、移動ＩＰの規定は、ネットワーク運用ポリシーを考慮していないため、例えば、外部組織のネットワークに移動して移動ＩＰの登録メッセージをホームネットワーク宛に送信する場合、外部ネットワークのゲートウェイが外向きパケットをすべて許すのであれば、移動ＩＰの規定がそのまま使用できるが、一般にこれはセキュリティの観点から望ましくない。したがって、移動計算機は、自身が外部組織のネットワークにいる、ということを認識し、ゲートウェイに対して自分の身分証明を行う処理を行ってから外部アクセスを行うことが必要になるが、本発明によれば、移動計算機が自身の現在位置を認識して現在接続しているネットワークから外へのアクセスを行う場合に必要な処理を正しく実行できる。

【００７０】以上のように本発明にれば、例えば移動ＩＰによる移動計算機の制御とＩＰセキュリティによるパケット暗号化処理をあわせて適用した場合に、実際のシステムで運用する場合の各ネットワークの管理ポリシーを反映しかつ効率の良いシステム制御を実現できる。すなわち、本発明によれば、システム全体のネットワーク構成に依存せずに移動計算機制御方式とパケット暗号化方式の両者を適用した通信システムを実現できる。

【００７１】なお、以上の各装置に係る発明は、方法に係る説明としても成立する。

【００７２】また、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【００７３】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００７４】通信システム内を移動して通信を行うことが可能な計算機を移動計算機と呼び、通信システム内を移動せず固定の位置で通信を行う計算機を固定計算機と呼ぶ。

【００７５】ある移動計算機について、その移動計算機がホームポジションを持つネットワークのことをホームネットワークと呼び、ホームネットワーク以外のゲートウェイを有するネットワークを他部署ネットワークと呼ぶ。

【００７６】ホームネット内にいる（本来の位置の他に、ホームネット内で単にルータを越えた移動はしているが、ゲートウェイを越えた移動はしていない場合を含む）移動計算機は、固定計算機と同様の扱いとなる。

【００７７】固定ノードは、ホームネット内にいる移動計算機と固定計算機を含む。

【００７８】また、ＧＷ保護域内とは、ゲートウェイで保護されているネットワーク（図１では、ホームネットワーク、他部署ネットワーク）を指す。ＧＷ保護域外とは、それ以外の外部を指す。後者の場合の計算機を外部ノードと呼ぶ。

【００７９】図１に、本実施形態に係る通信システムの基本構成の一例を示す。

【００８０】図１の通信システムは、先に図４２や図４３を参照しながら説明した移動ＩＰ、ＩＰセキュリティなどにより移動計算機の通信をサポートしているものとする。なお、移動ＩＰプロトコルでは、移動先ネットワークで移動計算機に対するパケット配送を行うフォーリンエージェントというルータの存在を仮定するモードと、フォーリンエージェントを設けない（移動先計算機自身がフォーリンエージェントを兼ねる）ポップアップモードがあるが、本実施形態では、ポップアップモード

を採用するものとして説明する。

【００８１】ところで、計算機間のパケット通信には、固定計算機間の通信、固定計算機・移動計算機間の通信、移動計算機間の通信の３つのケースが存在し得る。そして、ホームネット内に位置する移動計算機は固定ノードであるので、計算機間のパケット通信は、固定ノード間の通信、固定ノード・ホームネット外に移動中の移動計算機間の通信、ホームネット外に移動中の移動計算機間の通信の３つに分類できる。

【００８２】固定計算機間の通信と、固定計算機・ホームネット内に位置する移動計算機間の通信と、ホームネット内に位置する移動計算機間の通信とは、いずれも同様の制御手順となる。また、ホームネット外に移動中の移動計算機間の通信は、経路最適化前は固定ノードであるホームエージェントを介した通信になるので、ホームネット外に移動中の移動計算機と固定計算機との間の通信に帰結される。

【００８３】従って、本実施形態では、移動計算機（ＭＮ）２・通信相手計算機（ＣＨ）の間でのパケット転送について、通信相手計算機（ＣＨ）３を固定ノードとした場合を中心に説明し、その他に通信相手計算機（ＣＨ）３を移動計算機とした場合や固定計算機同士の通信について言及する。

【００８４】なお、本実施形態では、図１のネットワーク１ａの内部にホームポジションを持つ移動計算機（ＭＮ）２とその通信相手計算機（ＣＨ）３に関するパケット通信を中心にして説明を行うので、図１では、ネットワーク１ａをホームネットワーク、ネットワーク１ｂ，１ｃを他部署ホームネットワークとして示してある。

【００８５】さて、図１では、ホームネットワーク１ａ、第１の他部署ネットワーク１ｂ、第２の他部署ネットワーク１ｃがインターネット６を介して相互に接続されており、移動計算機（ＭＮ）２、移動計算機の通信相手（ＣＨ）３は、これらネットワーク内に接続され、または外部ノードとしてインターネット６に接続される。ネットワーク１ａ，１ｂ，１ｃには、入力パケットに所定のパケット処理を施して転送するパケット処理装置（すなわちパケット暗号化ゲートウェイ；以下ゲートウェイと呼ぶ；また、ＧＷはゲートウェイを表すものとする）４ａ，４ｂ，４ｃがそれぞれ設けられるものとする。ゲートウェイ４ａ，４ｂ，４ｃは、所定のセキュリティポリシーに従ってフィルタリングも行うが、本実施形態では、パケットが各ゲートウェイの通過条件を満たす場合について説明する（通過条件を満たさない場合はそのゲートウェイを通過できないだけである）。

【００８６】ホームネットワーク１ａには、移動ＩＰプロトコルをサポートするために、移動計算機の移動先の現在位置の情報を管理するホームエージェント（ＨＡ）５ａが設けられる。管理対象とする移動計算機の台数は任意である。前述したように、移動中の移動計算機２宛に転送されてきたＩＰパケットは、そのホームエージェント５を経由し、移動計算機２の元のアドレス（ホームネットワーク１ａにおけるアドレス）宛のＩＰパケットを移動ＩＰの現在位置アドレス宛パケット内にカプセル化することで、移動計算機２に対するデータの経路制御を行うことができる。なお、第１の他部署ネットワーク１ｂ、第２の他部署ネットワーク１ｃにも、必要に応じて、ホームエージェント５ｂ，５ｃが設けられる。また、後述する第３の他部署ネットワーク１ｄにも、同様の機能を持つホームエージェント５ｄが設けられる。

【００８７】本実施形態では、ゲートウェイ４ａ，４ｂ，４ｃは、パケット暗号化認証処理機能を持つものとする。また、移動計算機２は、少なくとも移動中には、パケット暗号化認証処理機能を持つものとする（図中、パケット暗号化認証処理機能を持つ移動計算機２をＭＮ＋で表す）。なお、パケット暗号化認証処理における通信データの暗号化／復号は、例えば、文献（ＩＥＴＦ ＲＦＣ１８２５，１８２７）に示される方式で実現できる。また、パケット暗号化認証処理における、認証データ（転送パケット内容と生成鍵から生成されるハッシュ関数値など）の付与／チェックは、例えば、文献（ＩＥＴＦ ＲＦＣ１８２５，１８２６）に示される方式で実現できる。

【００８８】なお、本実施形態では、固定計算機（特に外部ノードである固定計算機）はパケット暗号化認証処理機能を持たないものとして説明する（外部ノードである固定計算機がパケット暗号化認証処理機能を持つ場合については後に言及する）。

【００８９】本実施形態では、暗号／移動通信をサポートするため、パケット通信する計算機の位置、ゲートウェイの位置などに応じて、種々のフォーマットを持つパケット形式が使用される。

【００９０】図２に、ゲートウェイ、移動計算機で処理されるパケット形式を示す。

【００９１】（ａ）は、通常のＩＰパケット形式である。

【００９２】ＩＰヘッダには、通信を行う計算機の送信元のホーム・アドレスと宛先のホーム・アドレスが書込まれる。本実施形態では、ＩＰヘッダには、送信元となる計算機のアドレスと宛先となる移動計算機のアドレスが書込まれるものとする。

【００９３】（ｂ）は、移動ＩＰ形式であり、ホームエージェントで移動計算機宛に経路制御されるパケット形式である。

【００９４】先頭のＩＰヘッダには、送信元としてホームエージェントのアドレス、宛先として移動計算機の現在位置のケア・オブ・アドレス（Ｃａｒｅ－ｏｆアドレス）が書込まれ、後続のＩＰヘッダには、送信元となる計算機のアドレスと宛先となる移動計算機のホーム・アドレス（プライベート・アドレス（Ｐｒｉｖａｔｅアド

レス））が書込まれるものとする。

【００９５】（ｃ）は、暗号化／末端認証形式であり、末端のゲートウェイ間または末端のゲートウェイ～移動計算機間でパケットの暗号化および認証を行う形式である。

【００９６】末端間認証／暗号化情報のＩＰヘッダには、暗号化／認証を行う末端ノードの送信元アドレスと宛先アドレスが書込まれる。

【００９７】ＫＥＹ情報（鍵情報ヘッダ）は、受信側が認証処理に使用する鍵と復号処理に使用する鍵を得るための情報を含むヘッダ情報である。例えば、上記鍵をパケット処理鍵から生成する場合、ＩＰヘッダの送信元ノードと宛先ノードとの間で共有されるマスター鍵で暗号化されたパケット処理鍵が書込まれる。その他、必要に応じて、認証アルゴリズム、データの暗号化アルゴリズム、鍵暗号アルゴリズムを指定するための情報が書込まれる。

【００９８】ＡＨ情報（認証ヘッダ）は、所定の鍵（例えば、上記パケット生成鍵から生成した認証鍵）を使って生成された認証データを含むヘッダ情報である。

【００９９】ＥＳＰ情報（暗号化ヘッダ）は、所定の鍵（例えば、上記パケット生成鍵から生成した暗号鍵）を使って暗号化された内部データ（ここでは、内部ＩＰヘッダとそのデータ部）を復号するアルゴリズムを指定する情報を含むヘッダ情報である。

【０１００】内部ＩＰプロトコルは、カプセル化されたパケットであり、通信を行う計算機の送信元アドレスと宛先アドレスを含む内部ＩＰヘッダやそのデータ部からなる。例えば、上記（ａ）のパケットや上記（ｂ）のパケットに該当する。

【０１０１】（ｄ）は、暗号化／経路間認証形式である。途中経路間でのゲートウェイ間、途中経路のゲートウェイ～移動計算機間の認証を必要とする場合にはこの形式を使用する。

【０１０２】末端間認証／暗号化情報の部分、内部プロトコルの部分は、上記（ｃ）の場合と同様である。

【０１０３】経路間認証情報のＩＰヘッダには、認証を行うノードの送信元アドレスと宛先アドレスが書込まれる。

【０１０４】ＫＥＹ情報（鍵情報ヘッダ）は、受信側が認証処理に使用する鍵を得るための情報を含むヘッダ情報である。例えば、上記と同様、上記鍵をパケット処理鍵から生成する場合、ＩＰヘッダの送信元ノードと宛先ノードとの間で共有されるマスター鍵で暗号化されたパケット処理鍵が書込まれ、その他、必要に応じて、認証アルゴリズム、鍵暗号アルゴリズムを指定するための情報が書込まれる。

【０１０５】ＡＨ情報（認証ヘッダ）は、所定の鍵（例えば、上記パケット生成鍵から生成した認証鍵）を使って生成された認証データを含むヘッダ情報である。

【０１０６】なお、（ｃ）の暗号化／末端認証形式と、（ｄ）の暗号化／経路間認証形式では、いずれかの平文のヘッダ内に、送信元計算機のアドレスの情報と宛先計算機のアドレスの情報とを書込んで置くのが望ましい。

【０１０７】また、ゲートウェイ、移動計算機が使用する認証データとして、例えば、転送パケット内容と生成鍵から生成される一方向ハッシュ関数値（例えば、Ｋｅｙｅｄ　ＭＤ５方式）などが利用できる。

【０１０８】また、２つのデータパケット暗号化装置間あるいはデータパケット暗号化装置と移動計算機の間で共有されるマスター鍵は、例えば、秘密鍵の交換や、公開鍵と秘密鍵による導出（例えば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ法）により生成することができる。

【０１０９】末端間での認証は、固定ノードを暗号化認証処理対象とするゲートウェイ間、移動計算機のホームネットのゲートウェイと、ホームネット外に移動中の当該移動計算機との間で行われる。

【０１１０】経路間の認証は、ゲートウェイを持つ他のネットワークに移動中の移動計算機と当該移動計算機のホームネット内のノードとの通信において当該計算機のホームネットのゲートウェイと当該計算機の移動先ネットのゲートウェイとの間、および当該移動計算機の送信するパケットをその移動先ネットのゲートウェイが認証なしに外部へ通過させない場合に当該移動計算機とその移動先ネットのゲートウェイ間で行われる。

【０１１１】各ゲートウェイは、上記のいずれかの形式で入力されたパケットを、同一形式あるいは形式を変換して転送する。その際、自装置が末端認証や経路間認証の宛先になっている場合には、認証チェックに成功した場合のみパケットを通過させる。また、自装置が末端認証や経路間認証の送信元になっている場合には、所定のヘッダ情報を付加し、あるいは所定のヘッダ情報を付け替えて送信する。なお、パケット転送にあたっては、必要に応じて内部データの復号／再暗号化を行う。

【０１１２】また、各計算機は、上記の移動ＩＰ形式以外のいずれかの形式でパケットを送信し、上記のいずれかの形式でパケットを受信する。自装置が末端認証の宛先になっている場合には、内部データの復号を行うとともに、認証チェックに成功した場合のみ内部データを受け入れる（例えば上位モジュールに渡す）。また、移動ＩＰ形式のパケットについては、デカプセル化を行う。

【０１１３】移動ＩＰ形式のパケットを転送するのは、基本的にはホームエージェントだけである（なお、後述する経路最適化の特殊なケースとしてゲートウェイの場合もある）。

【０１１４】次に、本実施形態では、ゲートウェイ４ａ，４ｂ，４ｃは、自装置が現在、暗号化認証処理対象とする計算機を認識する暗号化認証処理対象計算機認識部を持つ。例えば、通信システム内のいずれかの場所（分散していても良い）に、各ゲートウェイがどの計算

機を暗号化認証処理対象とするかを示す情報のデータベース（具体例としては各ゲートウェイのネットワークアドレスと、その暗号化認証処理対象となる計算機群のネットワークアドレスの対応情報）を管理するサーバ装置を設置し、移動計算機が該データベースを検索することにより実現できる。あるいは、各ゲートウェイが、自装置の暗号化認証処理対象となる計算機群のネットワークアドレスの情報を保持することで実現できる。

【０１１５】また、各移動計算機は、後述する位置認識部により上記データベースやゲートウェイへの問い合わせなどをすることにより、現在、自装置を暗号化認証処理対象とするゲートウェイを検索することができる。

【０１１６】また、本実施形態では、各ゲートウェイ４ａ，４ｂ，４ｃは、上記の暗号化認証処理対象計算機認識部の他に、自装置が管理対象とする送信元計算機を認識する管理対象計算機認識部を持つ。管理対象計算機認識部は、例えば、通信システム内のいずれかの場所（分散していても良い）に、各ゲートウェイがどの計算機を管理対象とするかを示す情報のデータベース（具体例としては各ゲートウェイのネットワークアドレスと、その管理対象となる計算機群のネットワークアドレスの対応情報）を管理するサーバ装置を設置し、移動計算機が該データベースを検索することにより実現できる。あるいは、各ゲートウェイが、自装置の管理対象となる計算機群のネットワークアドレスの情報を保持することで実現できる。

【０１１７】ゲートウェイ４ａ，４ｂ，４ｃは、ネットワーク内部の計算機から送信されたパケットが自装置の管理する計算機（例えば、当該ネットワーク内部をホームポジションとする計算機）から送信されたものである場合は、該パケットを認証チェックなしに（必要な処理を施した上で）外部へ通過させ、該パケットが自装置の管理しない計算機（例えば、一時的にそのネットワーク内に移動してきた計算機）から送信されたものである場合は、該パケット内に正当な認証データが含まれれば該パケットに必要な処理を施した上で通過させるが、該パケット内に正当な認証データが含まれなければ（該パケット内に認証データが含まれるが認証チェックで正当でないものと判断された場合、あるいは該パケット内に認証データ自体が含まれない場合）、該パケットの外部への通過を拒否する。

【０１１８】また、ゲートウェイ４ａ，４ｂ，４ｃは、パケットの転送を拒否された計算機から認証データを生成するために必要な鍵の情報を要求された場合には、要求メッセージから求められる該移動計算機のユーザに関する情報が所定の条件を満たすことを確認したならば、要求された鍵情報を返送する。

【０１１９】なお、ネットワークによっては、そのセキュリティポリシーに応じ、外部から移動してきた計算機の送信したパケットを認証チェックなしに外部へ通過させる場合も存在し得る。例えば、親しいネットワークから移動してきた移動計算機など、所定のものに限って管理対象として登録している場合、ネットワーク内部の計算機から送信されたパケットが自装置の管理する計算機から送信されたものか否かにかかわらず認証チェックなしに外部へ通過させる場合などが考えられる。

【０１２０】もし、あるネットワークにおいてネットワーク内部から認証チェックなしにすべてのパケットを外部へ通過させるセキュリティポリシーを採用する場合、そのネットワークのゲートウェイでは管理対象計算機認識部は不要となる。

【０１２１】以下では、移動計算機２が他部署ネットワーク１ｂに移動した場合に行われる処理について説明する。

【０１２２】まず、移動計算機２自身による現在位置検出、移動先ネットワークで使用するケア・オブ・アドレスの獲得などについて説明する。

【０１２３】移動計算機２は、自装置を管理するホームエージェント５ａの設置されたネットワーク（ホームネットワーク）１ａ外に位置することを認識する位置認識部を持つ。

【０１２４】図３に、位置認識部により移動計算機２の現在位置を検出する処理手順の一例を示す。

【０１２５】ここで、移動ＩＰの規定にあるように各ホームエージェントはその処理するサブネット内に定期的にエージェント広告メッセージをブロードキャストにより送出するものとする。また、各ゲートウェイは、各々が検査対象とする計算機のアドレスのリストを公開しており、ある計算機について、その送信パケットのチェックを司るゲートウェイを検索可能であるとする。

【０１２６】移動計算機２側では、まず、自装置がホームネットワーク１ａの内部に位置するか外に位置するかを判定する。自装置を管理するホームエージェント５ａの送出するエージェント広告メッセージを受信し、ホームネットワーク内部に位置するか外に位置するかを検知する。自装置の属するホームネットワーク１ａのホームエージェント５ａによるエージェント広告メッセージを受信した場合にはホームネットワーク１ａ内部に位置すると判定する。それ以外のホームエージェントによるエージェント広告メッセージを受信した場合、あるいはエージェント広告メッセージを受信できない場合にはホームネットワークの外に位置すると判定する（ステップＳ１１）。

【０１２７】移動計算機２は、自装置がホームネットワークの外に位置すると判定された場合（ステップＳ１２）、移動先のネットワーク（ここでは１ｂ）において、例えばＤＨＣＰやＰＰＰなどのプロトコルにより、移動先ネットワークで使用する移動ＩＰのケア・オブ・アドレスを取得する（ステップＳ１３）。

【０１２８】さらに、移動計算機２は、そのケア・オブ

・アドレスを保護する（暗号化認証処理対象とする）ゲートウェイ（ＧＷ＿ＭＨ）を検索する（ステップＳ１４）。

【０１２９】ここで、検索されたゲートウェイ（ＧＷ＿ＭＨ）とホームネットワークのゲートウェイが一致している場合（例えばホームネットワーク１ａ内で他のサブネットに移動した場合）には、自装置はホームドメイン内に位置すると判定する［ＭＮ－ｈｏｍｅ］。そうでない場合には、ホームドメイン外に位置すると判定する［ＭＮ－ｆｏｒｅｉｇｎ］。

【０１３０】なお、ホームドメイン内に位置すると判定された場合には、以下に示す一連の位置登録処理は実行せず、通常のＩＰパケット形式で登録要求を送る。

【０１３１】また、ケア・オブ・アドレスを保護するゲートウェイが存在しない場合、移動計算機２は外部ノードである。

【０１３２】なお、ケア・オブ・アドレスを取得した時点で、移動計算機２と、これを暗号化認証処理対象とするゲートウェイとの対応付けが所定のデータベース等に登録される。

【０１３３】次に、移動計算機がホームエージェントへ移動登録メッセージを通知する処理について説明する。

【０１３４】移動ＩＰ方式では、移動計算機が新規の移動先に移った場合、現在位置の情報を含む登録メッセージを、自装置を管理するホームエージェントに送ることが必要である。この場合、移動計算機がホームネットワークと親しいネットワークに移動して、そのゲートウェイが自装置の送信する登録メッセージやデータパケットを自由に外部に送出させる場合には、移動ＩＰの規定のままで動作が可能である。しかし、一般に移動計算機を外部から内部に滞在しているものとして扱うネットワークでは、セキュリティ上の考慮から、移動計算機の発するメッセージを自由に外部に送出させることは危険であることから、ゲートウェイは自装置が管理対象とする計算機以外の移動計算機の送信する登録メッセージやデータパケットを一旦通過拒否する。このような場合、移動計算機は、現在自装置を侵入者として扱うネットワークに位置することを認識し、そのゲートウェイとの間で身分証明に相当する手続きを行って外部アクセス許可を得た後に登録メッセージをホームエージェントへ送信することが必要になる。

【０１３５】ＩＥＴＦではＩＰパケットへの認証コード付与方式をＩＰセキュリティ標準（文献：ＩＥＴＦ　ＲＦＣ１８２６，１８２８）として規定しているが、この方法を利用し、移動計算機の身分証明のための処理としてデータパケットに移動計算機と移動先ネットワークのゲートウェイ間での認証データを付加し、ゲートウェイでは受信したパケットの認証コードを確認してから、外部にパケットを通過させるようにする。これによって、たとえ組織外のユーザが入って来てネットワーク外部に対しデータパケットを送信したいと要求しても、予め所定の方法で認証鍵を交換し身分保証を行った移動計算機のみに外部アクセスを許可することが可能となる。

【０１３６】さて、移動計算機２は、ケア・オブ・アドレスを獲得したら、ホームネットワーク１ａのホームエージェント５ａに現在位置の情報を含む登録メッセージを送信する。

【０１３７】まず、移動計算機２がホームドメインにいる［ＭＮ－ｈｏｍｅ］の場合は、

・ホームエージェント（ＨＡ）のＩＰアドレス
・移動計算機（ＭＮ）のＩＰアドレス

を調べ、移動計算機を送信元、ホームエージェントを宛先とする通通常のＩＰパケット形式で登録要求を送り、ホームエージェントからのＩＰパケット形式の応答を受信するだけでよい。

【０１３８】なお、ここでは、ホームエージェントと移動計算機のＩＰアドレスは、ホームネットでのプライベート・アドレスとする。

【０１３９】次に、移動計算機２がホームドメイン外［ＭＮ－ｆｏｒｅｉｇｎ］に移動している場合について説明する。

【０１４０】移動計算機２がホームドメイン外［ＭＮ－ｆｏｒｅｉｇｎ］に移動している場合（図４）、まず、

・ホームネットワークのゲートウェイ（ＧＷ０）のｇｌｏｂａｌアドレス
・ホームネットワークのゲートウェイ（ＧＷ０）の公開鍵
・移動計算機（ＭＮ）のケア・オブ・アドレス、プライベート・アドレス
・ホームエージェント（ＨＡ）のプライベート・アドレス

を調べ、第１の登録メッセージを送る。

【０１４１】図５に第１の登録メッセージの一例を示す。

【０１４２】このメッセージは、前述した図２（ｃ）の暗号化／末端認証形式のパケットに該当する。

【０１４３】末端間認証／暗号化情報のＩＰヘッダでは、送信元を移動計算機（ＭＮ）２のケア・オブ・アドレス、宛先をゲートウェイ（ＧＷ０）４ａのグローバル・アドレスとする。

【０１４４】内部ＩＰヘッダ（登録要求）では、送信元を移動計算機（ＭＮ）のプライベート・アドレス、宛先をホームエージェント（ＨＡ）のプライベート・アドレスとする。

【０１４５】これに対し、移動計算機２がホームネットワーク１ａと親しいネットワークに移動して、そのゲートウェイが登録メッセージを自由に外部に送出させるような場合には、ゲートウェイ４ｂは認証チェックなしに登録メッセージを通過させるので、ゲートウェイ４ｂから移動計算機２へ受諾応答が返されるだけであるが、も

しゲートウェイ４ｂが、管理対象でない計算機から自装置宛でないパケットを受信したならば外部へのパケットの通過を拒否するような場合には、この登録メッセージの通過は拒否され、ゲートウェイ４ｂから移動計算機２へ通過拒否メッセージが返送される。

【０１４６】図６に、通過拒否メッセージの一例として、ＴＣＰ／ＩＰ通信のＩＣＭＰメッセージを拡張した形式で実現したものを示す。

【０１４７】このメッセージは、前述した図２（ａ）の通常のＩＰパケット形式に該当する。

【０１４８】ＩＰヘッダでは、送信元をゲートウェイ４ｂ（ＧＷ１）のグローバル・アドレス、宛先を移動計算機（ＭＮ）のケア・オブ・アドレスとする。

【０１４９】この場合は、移動計算機２は、通過拒否メッセージ中に含まれるゲートウェイ４ｂのグローバル・アドレスを用いて、ゲートウェイ４ｂに対し鍵要求メッセージを送信して、所定のプロトコルにより公開鍵の問い合わせを行う。

【０１５０】図７に、鍵要求メッセージの一例を示す。

【０１５１】このメッセージは、前述した図２（ａ）の通常のＩＰパケット形式に該当する。

【０１５２】ＩＰヘッダでは、送信元を移動計算機（ＭＮ）のケア・オブ・アドレス、宛先をゲートウェイ４ｂ（ＧＷ１）のグローバル・アドレスとする。

【０１５３】この鍵要求メッセージに対し、ゲートウェイ４ｂが公開鍵情報を渡すか否かの判断は、ゲートウェイ４ｂのサイトのシステム管理のポリシーに依存する。

【０１５４】例えば、

・鍵要求情報に所定の書式で付加されたユーザ識別情報を調べ、社内ユーザであれば、鍵情報を返す。

・社外ユーザであれば、所定の組織であれば鍵情報を渡す。

・それ以外の場合、予め登録されたユーザであれば、鍵情報を渡す。

といった規則をゲートウェイ４ｂに登録しておく。

【０１５５】ゲートウェイ４ｂに対するユーザ登録方法などはシステムの性質に応じ任意に設定すれば良い。

【０１５６】この鍵要求メッセージに対し、ゲートウェイ４ｂの公開鍵が得られたら、移動計算機２は、この鍵を使って生成した認証データを付加した２度目の登録要求を送る（なお、ゲートウェイ４ｂの管理対象でない計算機が、鍵情報を入手できなければ、この計算機は、ゲートウェイ４ｂから外にパケットを通過させることはできない）。

【０１５７】図８に、第２の登録メッセージの一例を示す。

【０１５８】このメッセージは、前述した図２（ｄ）の暗号化／経路間認証形式のパケットに該当する。

【０１５９】経路間認証情報のＩＰヘッダ１では、送信元を移動計算機（ＭＮ）２のケア・オブ・アドレス、宛先をゲートウェイ（ＧＷ１）４ｂのグローバル・アドレスとする。

【０１６０】末端間認証／暗号化情報のＩＰヘッダ２では、送信元を移動計算機（ＭＮ）２のケア・オブ・アドレス、宛先をゲートウェイ（ＧＷ０）４ａのグローバル・アドレスとする。

【０１６１】内部ＩＰヘッダ（登録要求）では、送信元を移動計算機（ＭＮ）のプライベート・アドレス、宛先をホームエージェント（ＨＡ）のプライベート・アドレスとする。

【０１６２】この第２の登録メッセージには、ゲートウェイ４ｂ宛でかつゲートウェイ４ｂに対する認証データを含むＡＨ情報（図２（ｄ）の経路間認証情報中のＡＨ情報）が付与されているので、ゲートウェイ４ｂは認証チェック処理を行い、これに成功すればメッセージは通過できる。

【０１６３】その際、ゲートウェイ４ｂは、次段のゲートウェイ４ａ宛に、図２（ｄ）の暗号化／経路間認証形式パケットで登録メッセージを転送する。

【０１６４】そして、登録メッセージは、インターネット６からゲートウェイ４ａを介してホームエージェント５ａに到着する。

【０１６５】登録メッセージが移動計算機２のホームネットワーク１ａのホームエージェント５ａに到着すると、その管理表には、移動計算機２の全ネットワーク中における位置を一意に特定可能な情報が登録される（この時点で、ホームエージェント５ａは、移動計算機２がホームネットワーク１ａ外に移動したことを認識する）。

【０１６６】また、例えば、ネットワーク１ａでは、ゲートウェイ４ｂの管理表に、インターネット６側からその移動計算機２宛に転送されてきたパケットをホームエージェント５ａに転送するように設定がなされる。これによって、インターネット６から移動計算機２のホームネットワーク１ａに転送されてきた移動計算機２宛のパケットは、一旦ホームエージェント５ａに渡され、ここから、移動計算機２の移動先に宛てて転送されるようになる。その際、ホームエージェント５ａにて、前述したように、移動計算機２の元のアドレス（ホームネットワーク１ａにおけるアドレス）宛のＩＰパケットを移動ＩＰ形式の現在位置アドレス宛パケット内にカプセル化する処理が行われる。あるいは、ホームエージェントがＭＮのｐｒｏｘｉｙ　ＡＲＰを行って、パケットを取るようにしても良い。

【０１６７】さて、登録メッセージを受けたホームエージェント５ａは、移動計算機２に対して、ホームエージェント５ａを送信元、移動計算機２を宛先とするＩＰ形式の登録応答メッセージを送信する。

【０１６８】ホームエージェント５ａから登録応答メッセージを受信すると、ゲートウェイ４ａは、このパケッ

トを図９に示すように次段のゲートウェイ４ｂ宛の暗号化／経路間認証形式にカプセル化して転送する。

【０１６９】経路間認証情報のＩＰヘッダ１では、送信元をゲートウェイ４ａ（ＧＷ０）のグローバル・アドレス、宛先をゲートウェイ４ｂ（ＧＷ１）のグローバル・アドレスとする。

【０１７０】末端間認証／暗号化情報のＩＰヘッダ２では、送信元をゲートウェイ４ａ（ＧＷ０）のグローバル・１アドレス、宛先を移動計算機（ＭＮ）のケア・オブ・アドレスとする。

【０１７１】内部ＩＰヘッダ（登録要求）では、送信元をホームエージェント（ＨＡ）のプライベート・アドレス、宛先を移動計算機（ＭＮ）のプライベート・アドレスとする。

【０１７２】このパケットがゲートウェイ４ｂに到達すると、ゲートウェイ４ｂでは、図１０に示すように暗号化／末端認証形式にして（ＩＰヘッダ１、ＫＥＹ１、ＡＨを取り除いて）移動計算機宛に転送する。

【０１７３】以上の登録処理が完了したら（登録メッセージに対して一旦転送拒否を示すメッセージを受信した後に鍵情報と認証データのやり取りによって応答受諾を受信した場合）、それ以降、移動計算機２がその移動中のネットワークの外部に位置する通信相手計算機３とデータ通信を行う場合も、上記の移動計算機２～ゲートウェイ４ｂ間の認証データをパケットに付加して転送する。本実施形態では、暗号化／経路間認証形式でパケットを送信する。この認証データ付加があるか否かによって、ゲートウェイ４ｂにて正しく認識されている訪問ノードであるか否かを正しく判定し、セキュリティに正しい移動計算機のメッセージ制御を行うことが可能となる。

【０１７４】なお、登録メッセージに対して転送拒否されずに応答受諾を受けた場合には、通信相手となる計算機３へのパケットを通常通り送信する。本実施形態では、暗号化／末端認証形式でパケットを送信する。

【０１７５】なお、移動計算機が外部ノードとして移動した場合には、移動計算機からホームエージェントへの登録メッセージは暗号化／末端認証形式で送信され、上記と異なり通過拒否なしにゲートウェイに転送され、ここでＩＰ形式にされホームエージェントに到達する。また、ホームエージェントから移動計算機への通常のＩＰ形式の応答メッセージはゲートウェイで暗号化／末端認証形式に変換され、移動計算機に到達する。以降、移動計算機２がその通信相手計算機３とデータ通信を行う場合も、暗号化／末端認証形式でパケットを送信する。

【０１７６】ここで、移動計算機がホームネット外に移動した場合、後のパケット転送でゲートウェイに必要な制御を行ってもらうために、当該移動計算機、ホームエージェントあるいはホームネットのゲートウェイなどにより、移動計算機のホームネットでのアドレスと、獲得したケア・オブ・アドレスの組を所定のデータベースに登録するようにする。このデータベースは、通信システム内のいずれかの場所に設置したサーバ装置に管理させ、あるいは各ゲートウェイに分散して管理させるなどし、各ゲートウエイから検索可能とする。

【０１７７】以下では、様々な位置関係にある計算機間でパケット通信が行われる場合の各ノードの動作や使用されるパケット形式等について説明する。

【０１７８】まず、計算機やゲートウェイがどのようなパケット形式でパケットを送受信するかについての基本的なプロトコルについて説明する。

【０１７９】この場合は、固定ノードとは、移動計算機でない固定計算機、ホームネット内に位置する移動計算機、ホームエージェントを含む。

【０１８０】また、各ネットワークは、ゲートウェイに保護されているものとする。

【０１８１】次のＰ０－１～Ｐ０－３は、パケット転送にゲートウェイが介在しない場合である。

【０１８２】（Ｐ０－１）送信元ノードが位置するネットワークと同一のネットワーク内に位置する固定ノードに対しては、送信元ノードから直接、通常のＩＰ形式パケットが転送される（図１９の通信相手ＣＨ・移動計算機ＭＮ、図２１の通信相手ＣＨ→ホームエージェントＨＡ、図２３の移動計算機ＭＮ→通信相手ＣＨ等参照）。

【０１８３】（Ｐ０－２）外部ノードである固定計算機同士は、直接、通常のＩＰ形式で通信するものとする。

【０１８４】（Ｐ０－３）外部ノードとして移動中の移動計算機同士は、経路最適化後は、直接、暗号化末端認証形式で通信する。

【０１８５】次のＰ２－１～Ｐ２－３は、通信する２台のノードが異なるネットワークに位置し、パケット転送に２台のゲートウェイが介在する場合である。

【０１８６】（Ｐ２－１）第１の固定ノードａから第２の固定ノードｂへのパケット転送が行われる場合（固定ノードａ→ＧＷａ→インターネット→ＧＷｂ→固定ノードｂ）

図１１に示すように、固定ノードａは通常のＩＰ形式でパケットを送信し、ＧＷａは該パケットを暗号化／末端認証形式にして転送し、ＧＷｂは該パケットをＩＰ形式にして転送する。末端認証は、ＧＷａ・ＧＷｂ間で行われる。

【０１８７】（Ｐ２－２）他部署ネットワークに移動中の移動計算機から固定ノードにパケットを転送する場合（移動計算機→ＧＷａ→インターネット→ＧＷｂ→固定ノード）

（ｉ）移動計算機が自装置の送信したパケットを認証なしには外部へ通過させない他部署ネットワークに位置する場合

図１２に示すように、移動計算機は暗号化／経路間認証形式でパケットを送信し、ＧＷａは該パケットを暗号化

／経路間認証形式にて転送し、ＧＷｂは該パケットをＩＰ形式にして転送する。末端認証は、移動計算機・ＧＷｂ間で行われる。経路間認証は、移動計算機・ＧＷａ間とＧＷａ・ＧＷｂ間で行われる。

【０１８８】（ii）移動計算機が自装置の送信したパケットを認証なしに外部へ通過させる他部署ネットワークに位置する場合

図１３に示すように、移動計算機は暗号化／末端認証形式でパケットを送信し、ＧＷａは該パケットを暗号化／経路間認証形式にして転送し、ＧＷｂは該パケットをＩＰ形式にして転送する。末端認証は、移動計算機・ＧＷｂ間で行われる。経路間認証は、ＧＷａ・ＧＷｂ間で行われる。

【０１８９】（Ｐ２－３）固定ノードから他部署ネットワークに移動中の移動計算機にパケットを転送する場合（固定ノード→ＧＷａ→インターネット→ＧＷｂ→移動計算機）

ホームエージェントは、パケットを転送する場合には移動ＩＰ形式で、登録応答メッセージを送信する場合には通常のＩＰ形式でパケットを送信する。また、経路最適化後において、移動計算機でない固定計算機またはホームに位置する移動計算機は、ＩＰ形式でパケットを送信する。

【０１９０】いずれの場合にも、ＧＷａはパケットを暗号化／経路間認証形式にて転送し、ＧＷｂは該パケットを暗号化／末端認証形式にして転送する。末端認証は、ＧＷａ・移動計算機間で行われる。経路間認証は、ＧＷａ・ＧＷｂ間で行われる。

【０１９１】図１４に、ホームエージェントがパケットを転送する場合について示す。

【０１９２】なお、ここでは、移動計算機が自装置の送信したパケットを認証なしには外部へ通過させない他部署ネットワークに位置する場合と、移動計算機が自装置の送信したパケットを認証なしに外部へ通過させる他部署ネットワークに位置する場合とで、同じの方法となる。

【０１９３】次のＰ１－１～Ｐ１－４は、パケット転送に１台のゲートウェイが介在する場合である。

【０１９４】（Ｐ１－１）外部ノードとして移動中の移動計算機からＧＷ保護域内に位置する固定ノードへの通信の場合（移動計算機→ＧＷ→固定ノード）

移動計算機は暗号化／末端認証形式でパケットを送信し、ＧＷは該パケットを通常のＩＰ形式にて転送する。末端認証は、移動計算機・ＧＷ間で行われる。

【０１９５】この場合を図１５に示す。

【０１９６】（Ｐ１－２）ＧＷ保護域内に位置する固定ノードから外部ノードとして移動中の移動計算機への通信の場合（固定ノード→ＧＷ→移動計算機）

ホームエージェントは、パケットを転送する場合には移動ＩＰ形式で、登録応答メッセージを送信する場合には

通常のＩＰ形式でパケットを送信する。また、経路最適化後において、移動計算機でない固定計算機またはホームに位置する移動計算機は、ＩＰ形式でパケットを送信する。

【０１９７】いずれの場合にも、ＧＷはパケットを暗号化／末端認証形式にして転送する。末端認証は、ＧＷ・移動計算機間で行われる。

【０１９８】この場合を図１５に示す。

【０１９９】（Ｐ１－３）固定計算機である外部ノードがＧＷ保護域内の固定ノードと通信する場合

この場合、暗号通信は行わないものとしているので、外部ノードとＧＷの間、ＧＷと固定ノードの間では、通常のＩＰ形式でパケット転送される。

【０２００】なお、固定計算機である外部ノードが暗号化認証機能を備えているならば暗号通信可能とするケースをサポートする場合、上記のＰ１－１、Ｐ１－２と同様の動作になる。

【０２０１】（Ｐ１－４）他部署ネットワークに移動中の移動計算機へ同一ネットワーク内の固定ノードからパケットを転送する場合で、かつ、経路最適化後の場合（固定ノード→ＧＷ→移動計算機）

固定ノードは通常のＩＰ形式でパケットを送信すると、ＧＷは該パケットを移動ＩＰ形式にして移動計算機に転送する。

【０２０２】次のＰｚ－１～Ｐｚ－３は、セキュリティーポリシーに応じて種々のケースが考えられる。

【０２０３】（Ｐｚ－１）外部ノードとして移動中の移動計算機が固定計算機である外部ノードと通信しようとする場合

後述するように、ホームネットワークのプロキシーを介した通信とする。

【０２０４】従って、移動計算機とゲートウェイの間でのパケット通信には暗号化／末端認証形式が使用され、固定計算機とゲートウェイの間でのパケット通信には通常のＩＰが使用される。

【０２０５】（Ｐｚ－２）他部署ネットワークに移動中の移動計算機が固定計算機である外部ノードと通信しようとする場合

暗号通信を行わないものとする。

【０２０６】（Ｐｚ－３）上記のＰｚ－２で、経路最適化する場合

移動計算機と固定計算機は、暗号通信を行わずに、ゲートウェイを介して直接通信するものとする。

【０２０７】なお、Ｐｚ－２とＰｚ－３において、移動計算機から固定計算機宛のパケットのみ、ゲートウェイを通過させるために移動計算機・ゲートウェイ間で認証を行っても良い（例えば暗号化／末端認証形式を使用する）。

【０２０８】上記のプロトコルを送信元となる計算機についてまとめると、次のようになる。

【０２０９】・固定計算機は、常に通常のＩＰ形式のパケットを送信する。

【０２１０】・ホームエージェントは、移動計算機へのパケット転送を行う場合、移動ＩＰ形式を使用する。ただし、登録応答メッセージは、ＩＰ形式での送信となる。

【０２１１】・移動計算機は、自装置の位置する場所を認識した結果により、以下のように動作が異なってくる。

【０２１２】（Ｓ１）自装置がホームに位置する場合、通常のＩＰ形式のパケットを送信する。

【０２１３】（Ｓ２）自装置が現在位置するネットワーク内に宛先計算機が位置すると認識された場合、通常のＩＰ形式のパケットを送信する。

（Ｓ３）移動先のネットワークのゲートウェイが自装置の送信するパケットを認証した後に外部へ通過させる場合、宛先計算機がその移動先ネットワークの外部に位置するとき、暗号化／経路間認証形式のパケットを送信する。

（Ｓ４）移動先のネットワークのゲートウェイが自装置の送信するパケットを認証なしに外部へ通過させる場合、宛先計算機がその移動先ネットワークの外部に位置するとき、暗号化／末端認証形式のパケットを送信する。

（Ｓ５）自装置が現在外部ノードとして移動している場合、暗号化／末端認証形式のパケットを送信する。

【０２１４】（Ｓ６）ただし、Ｓ４とＳ５において、相手計算機が外部ノードである固定計算機の場合、上記のＰｚ－２やＰｚ－３の手順によっては、相手計算機が外部ノードである固定計算機であるか否かに応じて、パケット形式を選択する場合がある。すなわち、Ｐｚ－２とＰｚ－３において、移動計算機・ゲートウェイ間で認証を行わない場合、通常のＩＰ形式を使用する（例外処理となる）。一方、移動計算機・ゲートウェイ間で認証を行う場合、暗号化／末端認証形式を使用する。後者の場合、Ｓ４とＳ５において、相手計算機が外部ノードである固定計算機であるか否かにかかわらず、パケット形式は統一される。

【０２１５】移動計算機は、図３で説明した位置認識部により、自装置の現在位置が、ホームネット内部か、ホームネット外部か、外部ノードかを認識することができる。また、外部ノードでない場合、自装置を現在、暗号化認証処理対象とするゲートウェイを知ることができる。

【０２１６】また、移動計算機は、通信相手の現在の位置を認識する通信相手位置認識部を持つ。例えば、前述した各ゲートウェイについてそれが暗号化認証処理対象とする計算機の情報を登録したデータベースを検索することにより実現できる。

【０２１７】なお、通信相手が移動計算機でホームネット外に移動中の場合、移動計算機のホームネットでのアドレスをもとに検索等を行うので、移動計算機のホームネットのゲートウェイが認識される。

【０２１８】図１６に、通信相手の位置を検出する処理の一例を示す。

【０２１９】通信相手のＩＰアドレスから対応するアドレスを保護域とするゲートウェイ（ＧＷ＿通信相手ＣＨ）を検索する（ステップＳ２１）。検索にかからなければ通信相手はＧＷ保護域外であると認識する。

【０２２０】通信相手がＧＷ保護域内の場合（ただしそのゲートウェイが自装置を現在、暗号化処理対象とするゲートウェイと異なる場合）、後のデータ通信で必要となるので、通信相手のホームネットのゲートウェイの暗号化／認証用公開鍵を取得する（ステップＳ２３）。例えば、自装置のホームネットワークのゲートウェイもしくは別途設置した管理サーバに問い合わせる。なお、該当する鍵を既に持っている場合にはこの手続きは不要である。

【０２２１】なお、上記の（Ｓ３）と（Ｓ４）について、移動先のネットワークのゲートウェイが自装置の送信するパケットを認証した後に外部へ通過させるか、認証なしに外部へ通過させるかは、前述した登録メッセージに関する手順を行った結果から知ることができる。すなわち、暗号化／末端認証形式で送信した登録メッセージに対して通過拒否された場合は（Ｓ３）に該当し、暗号化／末端認証形式で送信した登録メッセージが受諾され通過された場合は（Ｓ４）に該当する。

【０２２２】次に、各ゲートウェイは、種々の条件に応じて、ある形式のパケットを、そのまま、あるいは同じ形式で内容を変えてあるいは、あるいは異なる形式に変換して転送する。

【０２２３】各ゲートウェイは、入力パケットのヘッダ情報から送信元となる計算機や宛先となる計算機の情報を読取り、この情報をもとに所定のデータベース等を検索するなどして、必要な情報を得ることができる。

【０２２４】各ゲートウェイは、パケットの転送に係る計算機が、ホームネット外に移動中の移動計算機か否かを認識する移動計算機認識部と、パケットの転送に係る計算機について、これを暗号化処理対象とする計算機を認識するゲートウェイ認識部とを備える。また、前述したように、自装置が現在、暗号化認証処理対象とする計算機を認識する暗号化認証処理対象計算機認識部を持つ。

【０２２５】移動計算機認識部は、例えば、前述したホームネット外に移動中の移動計算機に関する登録を行ったデータベースを検索することにより実現できる。

【０２２６】ゲートウェイ認識部は、前述した移動計算機の通信相手位置認識部と同様で、各ゲートウェイについてそれが暗号化認証処理対象とする計算機の情報を登録したデータベースを検索することにより実現できる。

【０２２７】なお、通信相手がＧＷ保護域内の場合（ただしそのゲートウェイが自装置を現在、暗号化処理対象とするゲートウェイと異なる場合）、後のデータ通信で必要となるので、通信相手のホームネットのゲートウェイの暗号化／認証用公開鍵を取得する。例えば、自装置のホームネットワークのゲートウェイもしくは別途設置した管理サーバに問い合わせる。なお、該当する鍵を既に持っている場合にはこの手続きは不要である。

【０２２８】。

【０２２９】また、ゲートウェイは、計算機等から経路最適化の要求を受けた場合あるいは自発的に、移動計算機認識部やゲートウェイ認識部による認識結果をもとにして、経路最適化が可能か否かを判定するとともに、経路最適化が可能で自装置が経路最適化に寄与するものと認識された場合、認識結果に応じた経路を最適化するための制御を行う経路最適化制御部を備えても良い。

【０２３０】経路最適化制御部では、最適化前でのパケットに対する処理内容を、最適化後でのパケットに対する処理内容に変更する。

【０２３１】ここで、ゲートウェイと計算機がパケット処理のために用いるホームネット外に移動中の移動計算機や固定計算機の位置情報（各計算機を保護するゲートウェイの情報）の管理についてさらに説明する。

【０２３２】各計算機の位置情報は、各々の計算機自身が発して他のノードに通知するように構成することが可能である。

【０２３３】この場合、位置情報の通知方式としては、例えば、以下の２つの方法が考えられる。

【０２３４】（１）データベースで管理する方法

各計算機が夫々現在の位置情報（自装置を暗号化処理対象とするゲートウェイのアドレス情報）を中央のデータベースに報告し、以降、その情報が必要なノードは、そのデータベースに問い合わせを行って処理を進める。データベースはシステム内の任意の位置に置いて構わないが、移動計算機がホームネット外に移動した際に情報が更新される点を考慮すると、例えば、移動計算機のホームネットワーク内の移動計算機位置情報管理装置内に置くのが便利である。

【０２３５】（２）データ転送に伴って、経路途中の構成要素に通知する方法

各計算機が最初のデータを転送する際に、そのデータパケットの一部分に自身の位置情報を入れ、これを経路途中のノードが取り出して、当該ノードの持つ位置情報キャッシュに格納する。この方法は、位置情報を一元管理できないが、データ転送に伴って位置情報を伝搬でき、別のアクセスが不要になるので効率の点では有利である。

【０２３６】さて、ゲートウェイは、前述の移動計算機認識部やゲートウェイ認識部による認識結果に応じて、計算機間での通信にどのようなプロトコルが適用されるのかを判断し、また入力パケットをどのように処理して転送するかを判断し、例えば以下に示すような所定の処理を行う。

【０２３７】（Ｇ１）パケット転送を行ういずれの計算機も固定ノードであり、かつ、いずれの計算機についてもゲートウェイの存在が確認された場合、ゲートウェイは、通常のＩＰ形式が来たら、暗号／末端認証形式にカプセル化し、暗号／末端認証形式が来たら、通常のＩＰ形式にデカプセル化する。末端認証はゲートウェイ間で行う。

【０２３８】（Ｇ２）少なくとも一方の計算機が、ホームネット外に移動中の移動計算機で、かつ、いずれの計算機も自装置を暗号化認証処理対象とするゲートウェイを持たない固定ノードではないことが認識された場合は、以下のようになる。

【０２３９】（ｉ）通常のＩＰ形式が来たら、暗号／末端認証形式にカプセル化し、暗号／末端認証形式が来たら、通常のＩＰ形式にデカプセル化する（経路最適化に係るゲートウェイを除く）。末端認証はゲートウェイ間で行う。

【０２４０】ただし、次の２つは例外処理となる（例えば、ヘッダ情報から制御メッセージであることを認識して処理を行う）。

【０２４１】ホームエージェント発、ホームネット外に移動中で自装置を暗号化認証処理対象とするゲートウェイを持たない移動計算機宛のＩＰ形式のパケット（例えば、登録確認メッセージ）については、末端認証はゲートウェイ・移動計算機間で行う。

【０２４２】また、ホームエージェント発、ホームネット外に移動中で自装置を暗号化認証処理対象とするゲートウェイを持つ移動計算機宛のＩＰ形式のパケット（例えば、登録確認メッセージ）については、暗号／経路間認証形式にカプセル化して転送する。末端認証はゲートウェイ・移動計算期間で行い、経路間認証はゲートウェイ間で行う。

【０２４３】（ii）ホームネット外に移動中の移動計算機（自装置が暗号化認証処理対象とするもの）発の暗号化／末端認証形式パケットまたは暗号化／経路間認証形式パケットが来たら、暗号化／経路間認証形先パケットを次段に転送する。

【０２４４】（iii）次段が外部から移動中の移動計算機（自装置が暗号化認証処理対象とするもの）である、暗号化／経路間認証形式パケットが来たら、暗号化／末端認証形式パケットを転送する。

（iv）次段が固定ノードである（自装置を末端認証の受信側とする）暗号化／末端認証形式パケットまたは暗号化／経路間認証形式パケットが来たら、デカプセル化してＩＰ形式のパケットを転送する。

【０２４５】（ｖ）移動ＩＰ形式のパケットが来たら、宛先計算機がホームネット外に移動中の計算機であり、

かつこの計算機を暗号化認証処理対象とするゲートウェイが存在する場合、暗号化／経路間認証形式パケットにして転送し、宛先計算機がホームネット外に移動中の計算機であり、かつこの計算機を暗号化認証処理対象とするゲートウェイが存在しない場合、暗号化／末端認証形式パケットにして転送する。

【０２４６】（vi）経路最適化に係るゲートウェイは、経路最適化の要求を契機とし、例外処理として各ケースに応じた処理を行う。

【０２４７】（Ｇ３）一方の計算機が固定計算機、他方の計算機がホームネット外に移動中の計算機で、かついずれの計算機も自装置を暗号化認証処理対象とするゲートウェイを持たない場合、固定計算機を送信元または宛先とする通常のＩＰ形式のパケットが来たら、通常のＩＰ形式のパケットを転送し、移動計算機を宛先とするＩＰ形式または移動ＩＰ形式のパケットが来たら、暗号化／末端認証形式のパケットにして転送し、暗号化／末端認証形式のパケットが来たら、通常のＩＰ形式のパケットにして転送する。

【０２４８】（Ｇ４）一方の計算機が固定計算機で、この計算機を暗号化認証処理対象とするゲートウェイが存在せず、かつ、他方の計算機を暗号化認証処理対象とするゲートウェイが存在する場合、入力したパケットと同一形式で、パケットを転送する。

【０２４９】ただし、他方の移動計算機の移動先のゲートウェイが、一方の計算機が固定計算機でかつこの計算機を暗号化認証処理対象とするゲートウェイが存在しないときでも、認証なしにはパケットを通過させないようにするセキュリティ・ポリシーを採用する場合、移動計算機は、当該ゲートウェイとの間での認証コードを付加してパケットを送信し（例えば、暗号化／末端認証形式を用いる）、当該ゲートウェイは、認証チェックに成功したならば、ＩＰ形式のパケットを転送する。その他では、入力したパケットと同一形式で、パケットを転送する。

【０２５０】以下では、図１のネットワーク１ａの内部にホームポジションを持つ移動計算機（移動計算機ＭＮ）２と固定ホストである通信相手計算機（通信相手ＣＨ）３とのパケット通信を例にとってより具体的に説明する。

【０２５１】まず、図１に示す通信システムにおいて、移動計算機２と固定ホストである通信相手３の存在する場所の組合せおよびその際の通信処理内容は、図１７のように［ケース１］～［ケース４］の４つのケースに大分類される。

【０２５２】［ケース１］移動計算機ＭＮがＧＷ保護域内、通信相手計算機通信相手ＣＨがＧＷ保護域内であるケース

［ケース２］移動計算機ＭＮがＧＷ保護域外、通信相手計算機通信相手ＣＨがＧＷ保護域内であるケース

［ケース３］移動計算機ＭＮがＧＷ保護域内、通信相手計算機通信相手ＣＨがＧＷ保護域外であるケース

［ケース４］移動計算機ＭＮがＧＷ保護域外、通信相手計算機通信相手ＣＨがＧＷ保護域外であるケース

さらに、上記の［ケース１］［ケース２］のゲートウェイＧＷを介した通信のケースを細分類すると、図１８に示すように、（ケース１）～（ケース７）の７つのケースに分類される（［ケース１］が（ケース１）～（ケース５）に細分類され、［ケース２］が（ケース６）と（ケース７）に細分類される）。

【０２５３】（ケース１）移動計算機ＭＮはホームネット内、通信相手計算機通信相手ＣＨも移動計算機ＭＮのホームネット内に位置するケース

（ケース２）移動計算機ＭＮはホームネット内、通信相手計算機通信相手ＣＨは他部署ネット内に位置するケース

（ケース３）移動計算機ＭＮは他部署ネット内、通信相手計算機通信相手ＣＨは移動計算機ＭＮのホームネット内に位置するケース

（ケース４）移動計算機ＭＮは他部署ネット内、通信相手計算機通信相手ＣＨも移動計算機ＭＮと同じネット内に位置するケース

（ケース５）移動計算機ＭＮはいずれかの他部署ネット内、通信相手計算機通信相手ＣＨは移動計算機ＭＮと異なる他部署ネット内に位置するケース

（ケース６）移動計算機ＭＮは外部ノード、通信相手計算機通信相手ＣＨは移動計算機ＭＮのホームネット内に位置するケース

（ケース７）移動計算機ＭＮは外部ノード、通信相手計算機通信相手ＣＨは他部署ネット内に位置するケース

各々のケースについて、各ノードの処理、各ゲートウェイでのＩＰセキュリティ処理が異なることがある。前述したように、通信相手３の位置によっては、暗号通信を使用できない場合もある。例えば、通信相手３がパケット暗号化認証処理を行うパケット処理装置のないネットワークにいる場合である。これは上の［ケース３］［ケース４］の場合に相当する。このような場合は、移動計算機は、移動ＩＰプロトコルのみを使用し、パケットの暗号化を行わないことになる。または、通常のＩＰ通信のみで、移動処理も行わないようにしても良い。

【０２５４】また、移動ＩＰでは、ホームエージェント経由の移動計算機宛のパケット経路を、各ネットワーク構成要素が正しい位置情報をキャッシュして保持している場合に最適化することを規定している。この経路最適化も、パケット暗号化を併用する場合、移動計算機と通信相手の現在位置を認識して、適用可能性を判定することが必要になる。

【０２５５】以上のように、移動ＩＰ、ＩＰセキュリティの併用する際には移動計算機、通信相手の位置情報を検出し、上記（ケース１）～（ケース７）と上記［ケー

ス３］［ケース４］のように通信相手がＧＷ保護域外にいるケースを認識するなどして、各ネットワーク構成要素の処理を制御することが非常に重要になる。

【０２５６】以下、上記の（ケース１）～（ケース７）、［ケース３］、［ケース４］の各ケースごとに説明を行う。

【０２５７】（ケース１）移動計算機ＭＮと通信相手ＣＨがともにホームネット１ａに位置する場合

この場合、移動計算機は固定ノードであるので、前述のＰ０－１に該当する。

【０２５８】また、移動計算機が送信するバケットの形式は、前述のＳ１とＳ２に該当する（いずれの判断によっても良い）。

【０２５９】図１９に示すように、移動計算機ＭＮと通信相手ＣＨは通常のＩＰバケット形式で直接通信する。

【０２６０】なお、ゲートウェイは介在しないので処理を行わない。

【０２６１】（ケース２）移動計算機ＭＮはホームネット１ａ、通信相手ＣＨが他部署ネット１ｂの場合

この場合、移動計算機は固定ノードであるので、前述のＰ２－１に該当する。

【０２６２】また、移動計算機が送信するバケットの形式は、前述のＳ１に該当する。

【０２６３】図２０に示すように、移動計算機ＭＮは通常のＩＰバケット形式を送出する。

【０２６４】ゲートウェイでは、ＩＰバケット形式が来たら、暗号／末端認証形式にカプセル化し、暗号／末端認証形式が来たら、ＩＰバケット形式にデカプセル化する。

【０２６５】（ケース３）移動計算機ＭＮは他部署、通信相手ＣＨがホームネットの場合

この場合、移動計算機ＭＮ→通信相手ＣＨがＰ２－２に該当し、通信相手ＣＨ→ホームエージェントＨＡがＰ０－１に該当し、ホームエージェントＨＡ→移動計算機ＭＮがＰ２－３に該当する。

【０２６６】また、移動計算機が送信するバケットの形式は、前述のＳ３またはＳ４のいずれかに該当する。

【０２６７】Ｐ２－３（ｉ）の場合を、図２１に示す。

【０２６８】図２２に示すように、移動計算機ＭＮは暗号化／経路間認証形式のバケットを送信する。

【０２６９】各ゲートウェイでは、以下のバケット処理を行う。

【０２７０】・移動計算機ＭＮ発の暗号化／経路間認証形式バケットが来たら、暗号化／経路間認証形先バケットを次段に転送する。

・次段が移動計算機ＭＮの、暗号化／経路間認証形式バケットが来たら、暗号化／末端認証形式バケットを転送する。

・それ以外の暗号化／経路間認証形式バケットが来たら、デカプセル化してＩＰ形式バケットを転送する。

・移動ＩＰ形式のバケットが来たら、暗号化／経路間認証形式バケットにして転送する。

【０２７１】（ケース４）移動計算機ＭＮと通信相手ＣＨは同一の他部署の場合

この場合、移動計算機ＭＮ→通信相手ＣＨがＰ０－１に該当し、通信相手ＣＨ→ホームエージェントＨＡがＰ２－１に該当し、ホームエージェントＨＡ→移動計算機ＭＮがＰ２－３に該当する。

【０２７２】また、移動計算機が送信するバケットの形式は、前述のＳ２に該当する。

【０２７３】Ｐ２－３（１）の場合を、図２３に示す。

【０２７４】図２４に示すように、移動計算機ＭＮは通常のＩＰバケット形式を送出する。

【０２７５】ゲートウェイでは、以下のバケット処理を行う。

【０２７６】・ＩＰバケット形式が来たら、暗号／末端認証形式バケットを転送する。

・暗号／末端認証形式バケットが来たら、デカプセル化してＩＰ形式バケットを転送する。

・移動ＩＰ形式バケットが来たら、暗号化／経路間認証形式バケットを転送する。

・次段が移動計算機ＭＮの、暗号化／経路間認証形式バケットが来たら、暗号／末端認証形式バケットを転送する。

【０２７７】ここで、経路最適化が要求された場合は、図２５に示すように、該当するゲートウェイは、通信相手ＣＨからのＩＰ形式バケットを受信したら、移動ＩＰ形式バケットを移動計算機ＭＮに転送するように制御する（Ｐ１－４に該当）。

【０２７８】（ケース５）移動計算機ＭＮは他部署、通信相手ＣＨは別の他部署の場合

この場合、移動計算機ＭＮ→通信相手ＣＨがＰ２－２に該当し、通信相手ＣＨ→ホームエージェントＨＡがＰ２－１に該当し、ホームエージェントＨＡ→移動計算機ＭＮがＰ２－３に該当する。

【０２７９】また、移動計算機が送信するバケットの形式は、前述のＳ３またはＳ４に該当する。

【０２８０】Ｐ２－３（ｉ）の場合を、図２６に示す。

【０２８１】図２７に示すように、移動計算機ＭＮは暗号化／経路間認証形式のバケット形式を送出する。

【０２８２】ゲートウェイでは、以下のバケット処理を行う。

【０２８３】・ＩＰバケットが来たら、暗号化／末端認証形式バケットを転送する。

・暗号化／末端認証形式バケットが来たら、デカプセル化してＩＰバケットを転送する。

・移動ＩＰバケット形式が来たら、暗号化／経路間認証形式バケットを転送する。

・移動計算機ＭＮ発の、暗号化／経路間認証形式バケットが来たら、暗号化／経路間認証形式バケットを転送す

る。
・次段が移動計算機ＭＮの、暗号化／経路間認証形式パケットが来たら、暗号化／末端認証形式パケットを転送する。
・それ以外の暗号化／経路間認証形式パケットが来たら、デカプセル化してＩＰ形式パケットを転送する。
【０２８４】ここで、経路最適化が要求された場合を、図２８に示す。
【０２８５】この場合、通信相手ＣＨ→移動計算機ＭＮがＰ２－３に該当する。
【０２８６】この場合、各ゲートウェイが以下のパケット処理を行うように制御する。
【０２８７】・移動計算機ＭＮ発の、暗号化／経路間認証形式パケットが来たら、暗号化／経路間認証形式パケットを転送する。
・次段が移動計算機ＭＮの、暗号化／経路間認証形式パケットが来たら、暗号化／認証形式パケットを転送する。
・それ以外の暗号化／経路間認証形式パケットが来たら、デカプセル化してＩＰ形式パケットを転送する。
【０２８８】・通信相手ＣＨからのＩＰ形式パケットが来たら、暗号化／経路間認証形式パケットを転送する。
【０２８９】（ケース６）移動計算機ＭＮは外部、通信相手ＣＨはホームの場合
この場合、移動計算機ＭＮ→通信相手ＣＨがＰ１－１に該当し、通信相手ＣＨ→ホームエージェントＨＡがＰ０－１に該当し、ホームエージェントＨＡ→移動計算機ＭＮがＰ１－２に該当する。
【０２９０】また、移動計算機が送信するパケットの形式は、前述のＳ５に該当する。
【０２９１】この場合を、図２９に示す。
【０２９２】図３０に示すように、移動計算機ＭＮは暗号化／末端認証形式のパケットを送出する。
【０２９３】ゲートウェイでは、以下のパケット処理を行う。
【０２９４】・暗号化／末端認証形式パケットが来たら、デカプセルしてＩＰパケットを転送する。
・移動ＩＰ形式が来たら、暗号化／経路間認証形式パケットを転送する。
【０２９５】（ケース７）移動計算機ＭＮは外部、通信相手ＣＨは他部署の場合
この場合、移動計算機ＭＮ→通信相手ＣＨがＰ１－１に該当し、通信相手ＣＨ→ホームエージェントＨＡがＰ２－１に該当し、ホームエージェントＨＡ→移動計算機ＭＮがＰ１－２に該当する。
【０２９６】また、移動計算機が送信するパケットの形式は、前述のＳ５に該当する。
【０２９７】この場合を、図３１に示す。
【０２９８】図３２に示すように、移動計算機ＭＮは暗号化／末端認証形式のパケット形式を送出する。
【０２９９】ゲートウェイでは、以下のパケット処理を行う。
【０３００】・ＩＰパケットが来たら、暗号化／末端認証形式パケットを転送する。
・暗号化／末端認証形式パケットが来たら、デカプセルしてＩＰパケットを転送する。
・移動ＩＰ形式が来たら、暗号化／末端認証形式パケットを転送する。
【０３０１】ここで、経路最適化が要求された場合を、図３３に示す。
【０３０２】この場合、通信相手ＣＨ→移動計算機ＭＮがＰ１－２に該当する。
【０３０３】この場合、各ゲートウェイが以下のパケット処理を行うように制御する。
【０３０４】・暗号化／末端認証形式パケットが来たら、デカプセルしＩＰパケットを転送する。
・通信相手ＣＨからのＩＰ形式パケットを受信したら、暗号化／末端認証形式パケットをＭＨに転送する。
【０３０５】（ケース８）通信相手ＣＨが保護域外、移動計算機ＭＮがホームの場合（上記［３］の場合）
図３４に示すように、通常のＩＰ通信のみを行う。
【０３０６】したがって、ゲートウェイでは暗号化認証処理は行わない。
【０３０７】（ケース９）通信相手ＣＨが保護域外、移動計算機ＭＮが外部の場合（上記［４］の場合）
図３５に示すように、通常の移動ＩＰ通信のみを行い、ゲートウェイでは暗号化は行わないものとする。
【０３０８】または、図３６に示すように、移動計算機ＭＮは移動先で得たケア・オブ・アドレスを使った通常のＩＰ通信を行い、移動ＩＰと暗号化は行わないようにしても良い。
【０３０９】なお、他部署ネットワーク１ｃのセキュリティ・ポリシーに応じて、図３５や図３６において、移動計算機２発のパケットをゲートウェイ４ｃから外部に転送する場合に、移動計算機２とゲートウェイ４ｃとの間でのみ、認証を行うようにしても良い。
【０３１０】（ケース１０）通信相手ＣＨが保護域外、移動計算機ＭＮが外部の場合（上記［４］の場合）
この場合を、図３７に示す。
【０３１１】以下のような処理を行うものとする。
【０３１２】・移動計算機ＭＮは一旦ホームドメインに向かって暗号化／末端認証形式でパケットを送信する（送信元アドレスはプライベート・アドレスとする）。
・ホームドメインのプロキシー１２でグローバル・アドレスに変換され、ＩＰパケットが外部に行く。
・帰りはプロキシー１２とホームエージェントＨＡを経由し、ゲートウェイ４ａから暗号化／末端認証形式で移動計算機ＭＮに届く。
【０３１３】以上では、図１のネットワーク１ａの内部にホームポジションを持つ移動計算機（移動計算機Ｍ

Ｎ）２と固定ホストである通信相手計算機（通信相手ＣＨ）３とのパケット通信を例にとってより具体的に説明した。

【０３１４】以下では、ホームネット外に移動中の計算機間でのパケット通信についてより具体的に説明する。

【０３１５】ホームネット外に移動中の計算機間でのパケット通信は、次の各ケースに分類される。

【０３１６】＜１＞２つの計算機ともＧＷ保護域内の場合

・異なるホームネットで、同じ他部署ネット（どちらのホームネットでもない）に位置するケース

・異なるホームネットで、異なる他部署ネット（どちらのホームネットでもない）に位置するケース

・異なるホームネットで、異なる他部署ネット（一方はいずれかのホームネット）に位置するケース

・異なるホームネットで、互いに通信相手のホームネットに位置するケース

・同じホームネットで、同じ他部署ネットに位置するケース

・同じホームネットで、異なる他部署ネットに位置するケース

・なお、上記の夫々のケースの夫々の他部署ネットについて、移動計算機の移動先ネットワークのゲートウェイが、自装置の装置するパケットを認証なしに外部へ通過させる場合と、そうでない場合がある。

【０３１７】＜２＞１つの計算機のみがＧＷ保護域内（他部署ネットと外部ノード）の場合

・ホームネットが異なる場合

・ホームネットが同じ場合

・なお、上記の夫々のケースの夫々の他部署ネットについて、移動計算機の移動先ネットワークのゲートウェイが、自装置の装置するパケットを認証なしに外部へ通過させる場合と、そうでない場合がある。

【０３１８】＜３＞２つの計算機ともＧＷ保護域外（外部ノード同士）の場合

・ホームネットが異なる場合

・ホームネットが同じ場合

以上の各ケースに分類されるが、前述したように、ホームネット外に移動中の計算機間でのパケット通信は、経路最適化前は、常に通信相手ＣＨのホームエージェントＨＡを介して行われるので、各計算機やゲートウェイの動作は、上記した移動計算機と固定計算機との通信の場合に帰結される。

【０３１９】以下では、上記の各ケースのうちのいくつかについてのみ（移動計算機の移動先ネットワークのゲートウェイが、自装置の装置するパケットを認証チェックした後に外部へ通過させる場合について）説明し、その他のケースについては容易に類推可能であるため説明を省略する。

【０３２０】なお、移動計算機は、通信相手のホームエージェントから発信される広告メッセージを受信した場合は、通信相手のホームネットに位置すると認識するものとする。

【０３２１】（Ｃ１）移動計算機ＭＮは他部署、通信相手ＣＨは別の他部署でいずれも通信相手ＣＨのホームエージェントＨＡとは異なる場所の場合

この場合を、図３８に示す。

【０３２２】図３９に示すように、各移動計算機は暗号化／経路間認証形式のパケット形式を送出する。

【０３２３】例えば、計算機２－１からのパケットは通信相手２－２が移動しているので、通信相手２－２のホームネットワーク１ｄのゲートウェイ４ｄに転送され、ここで一旦復号され、通信相手２－２のホームエージェント５ｄに送られる。このホームエージェント５ｄで移動ＩＰ形式のカプセル化が行われ、通信相手２－２の現在の位置に転送される。

【０３２４】すなわち、この場合の移動計算機２－１→通信相手２－２のホームエージェント４ｄの転送経路は、例えば、（ケース５）で示した移動計算機ＭＮ→通信相手ＣＨの転送経路における処理と同様になり、通信相手２－２のホームエージェント４ｄ→通信相手２－２の転送経路は、（ケース５）で示したホームエージェントＨＡ→移動計算機ＭＮの転送経路における処理と同様になる。

【０３２５】言い換えると、前者は先に説明したＰ２－２のケースに該当し、後者はＰ２－３のケースに該当する。

【０３２６】したがって、ゲートウェイでは、以下のパケット処理を行うことになる。

【０３２７】・移動ＩＰパケット形式が来たら、暗号化／経路間認証形式パケットを転送する。

・移動計算機ＭＮ発の、暗号化／経路間認証形式パケットが来たら、暗号化／経路間認証形式パケットを転送する。

・次段が移動計算機ＭＮの、暗号化／経路間認証形式パケットが来たら、暗号化／認証形式パケットを転送する。

・それ以外の暗号化／経路間認証形式パケットが来たら、デカプセル化してＩＰ形式パケットを転送する。

【０３２８】（Ｃ２）移動計算機ＭＮは他部署で通信相手ＣＨのホームエージェントＨＡが設置されたネット、通信相手ＣＨは別の他部署（どちらのホームエージェントＨＡもないネット）の場合

この場合を、図４０に示す。

【０３２９】計算機２－１を送信元とした場合は、図２１のＣＨケース３で通信相手３を送信元とする場合と同様になる。

【０３３０】計算機２－２を送信元とした場合は、上記のＣ１のケースと同様になる。

【０３３１】ゲートウェイでは、以下のパケット処理を

行うことになる。

【０３３２】・移動ＩＰパケット形式が来たら、暗号化／経路間認証形式パケットを転送する。

・移動計算機ＭＮ発の、暗号化／経路間認証形式パケットが来たら、暗号化／経路間認証形式パケットを転送する。

・次段が移動計算機ＭＮの、暗号化／経路間認証形式パケットが来たら、暗号化／認証形式パケットを転送する。

・それ以外の暗号化／経路間認証形式パケットが来たら、デカプセル化してＩＰ形式パケットを転送する。

【０３３３】したがって、ゲートウェイの処理は、上記のＣ１のケースと同様になる。

【０３３４】なお、上記の＜１＞のように２つの計算機ともＧＷ保護域内の場合、いずれのケースも、ゲートウェイはケース５の６種類の動作のうちの一部分を実行することになる。

【０３３５】次に、図４１に示すように、上記の＜２＞の１つの計算機のみがＧＷ保護域内（他部署ネットと外部ノード）のときに、２つの計算機が同じホームネットを持つ場合、先に説明したＧ２のケースにあるように、ゲートウェイは、ホームエージェント発、ホームネット外に移動中の計算機宛のパケットについて、宛先計算機に応じた処理を行う必要があるが、それ以外は、ケース５とケース６の動作のうちの一部分を実行することになる。

【０３３６】次に、上記の＜３＞のように、２つの計算機ともＧＷ保護域外（外部ノード同士）の場合、ゲートウェイは、ケース６の動作を実行することになる。

【０３３７】さて、従来、移動ＩＰ方式では、各ネットワークノードは一意なＩＰアドレスが付与され、自由に制御パケットをやりとりできるという仮定でのみ、経路制御や移動計算機位置の登録などの規定を行っていたが、本実施形態によれば、実際の運用に再して、移動計算機がどのような組織に属するネットワークに移動したか、というネットワーク運用ポリシーに関する動作規定を考慮することができる。

【０３３８】また、ＩＰセキュリティにもとづく暗号化装置を介して暗号化、認証通信を行う場合、各移動計算機、およびその通信相手の位置に応じて各ネットワーク構成要素の動作が大きく変化する。特に暗号化認証処理をともなって、移動ＩＰの経路最適化を行うためにも、この位置情報認識を有効に利用できる。

【０３３９】また、移動ＩＰの規定は、ネットワーク運用ポリシーを考慮していないため、例えば、外部組織のネットワークに移動して移動ＩＰの登録メッセージをホームネットワーク宛に送信する場合、外部ネットワークのゲートウェイが外向きパケットをすべて許すのであれば、移動ＩＰの規定がそのまま使用できるが、一般にこれはセキュリティの観点から望ましくない。したがって、移動計算機は、自身が外部組織のネットワークにいる、ということを認識し、ゲートウェイに対して自分の身分証明を行う処理を行ってから外部アクセスを行うことが必要になり、本発明によれば、移動計算機が自身の現在位置を認識して現在接続しているネットワークから外へのアクセスを行う場合に必要な処理を正しく実行できる。

【０３４０】以上のように、本実施形態により、移動ＩＰによる移動計算機の制御とＩＰセキュリティによるパケット暗号化処理をあわせて適用した場合に、実際のシステムで運用する場合の各ネットワークの管理ポリシーを反映し、かつ効率の良いシステム制御を実現できる。

【０３４１】なお、本実施形態では、固定計算機である外部ノードについては暗号通信をサポートしないものとして説明したが、固定計算機である外部ノードが暗号化認証機能を備えているならば暗号通信をサポートするようにしても良い。この場合、固定計算機である外部ノードのうち暗号化認証機能を備えているものを登録したデータベースをネットワーク中に設け、このデータベースを検索して固定計算機である外部ノードが暗号化認証機能を備えているならば、前述したＰ１－１（外部ノードとして移動中の移動計算機からＧＷ保護域内に位置する固定ノードへの通信の場合）、Ｐ１－２（ＧＷ保護域内に位置する固定ノードから外部ノードとして移動中の移動計算機への通信の場合）と同様の処理を行うようにしても良い。

【０３４２】また、上記した各例では、移動先ネットワークにおいてそのゲートウェイから一旦パケットの通過を拒否された場合、所定の手順の後、認証データをパケットに付加して送信するものであったが、その代わりに、ゲートウェイにて認証に成功した移動計算機を管理対象として管理テーブルに登録し、以降はその移動計算機については認証を省くようにしても良い（この場合、登録後は、移動計算機は認証データをパケットに付加せずに送信することができる）。

【０３４３】また、本実施形態では、パケット転送に介在するゲートウェイＧＷは最大で２台であってが、例えば計算機を処理対象とするＧＷａとＧＷｂとの間に、パケット転送に介在する他のＧＷｅが介在する場合には、ＧＷｅは暗号化／経路間認証形式以外のパケットを受信した場合、そのまま通過させるようにしても良い。また、暗号化／経路間認証形式のパケットを転送する場合、ＧＷａとＧＷｅ、ＧＷｅとＧＷｂとの間で、それぞれ、経路間認証を行うようにしても良い。

【０３４４】以上の各機能、例えば移動計算機に搭載するパケット暗号化認証部などは、ハードウェアとしてもソフトウェアとして実現可能である。また、上記した各手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体として実施することもできる。

【０３４５】なお、本実施形態では、ポップアップモードによる通信システムについて説明したが、本発明は、フォーリンエージェントの存在を仮定した通信システムにも適用可能である。

【０３４６】また、本発明は、現在種々提案されている移動通信プロトコル、暗号化通信プロトコル、暗号鍵交換プロトコルに対しても適用可能である。

【０３４７】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０３４８】

【発明の効果】本発明に係る移動計算機装置によれば、ネットワーク運用ポリシーを考慮し自装置の現在位置に応じた適正なパケット転送を行うことができる。

【０３４９】また、本発明に係るパケット処理装置によれば、ネットワーク運用ポリシーを考慮しパケット通信する計算機の現在位置に応じた適正なパケット転送、暗号化認証処理、経路最適化などの通信制御を行うことができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るシステムの基本構成の一例を示す図

【図２】同実施形態で使用するパケット形式の一例を示す図

【図３】同実施形態に係る移動計算機による自装置の位置判定処理の流れを示すフローチャート

【図４】同実施形態に係る移動登録メッセージ送信手順を説明するための図

【図５】同実施形態に係る第１の登録メッセージのフォーマットの一例を示す図

【図６】同実施形態に係る通過拒否メッセージのフォーマットの一例を示す図

【図７】同実施形態に係る鍵要求メッセージのフォーマットの一例を示す図

【図８】同実施形態に係る第２の登録メッセージのフォーマットの一例を示す図

【図９】同実施形態でゲートウェイ間を転送される登録応答メッセージのフォーマットの一例を示す図

【図１０】同実施形態で移動計算機が受信する登録応答メッセージのフォーマットの一例を示す図

【図１１】同実施形態に係るノード間の通信の一例を示す図

【図１２】同実施形態に係るノード間の通信の一例を示す図

【図１３】同実施形態に係るノード間の通信の一例を示す図

【図１４】同実施形態に係るノード間の通信の一例を示す図

【図１５】同実施形態に係るノード間の通信の一例を示す図

【図１６】同実施形態に係る移動計算機による通信相手の位置判定処理の流れを示すフローチャート

【図１７】通信態様の分類を説明するための図

【図１８】通信態様の分類を説明するための図

【図１９】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図２０】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図２１】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図２２】同実施形態で計算機の送信するパケット形式の一例を示す図

【図２３】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図２４】同実施形態で計算機の送信するパケット形式の一例を示す図

【図２５】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図２６】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図２７】同実施形態で計算機の送信するパケット形式の一例を示す図

【図２８】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図２９】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図３０】同実施形態で計算機の送信するパケット形式の一例を示す図

【図３１】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図３２】同実施形態で計算機の送信するパケット形式の一例を示す図

【図３３】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図３４】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図３５】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図３６】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図３７】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図３８】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

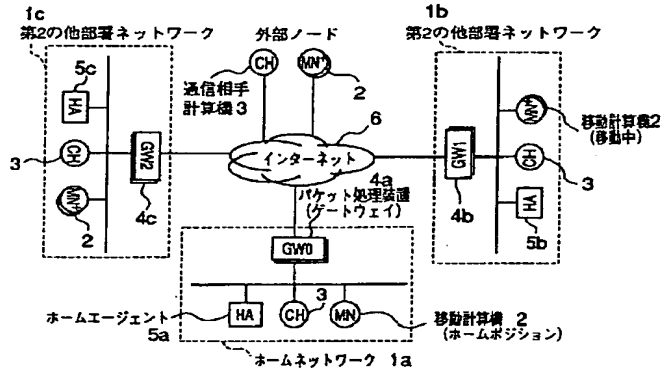
【図３９】同実施形態で計算機の送信するパケット形式の一例を示す図

【図４０】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

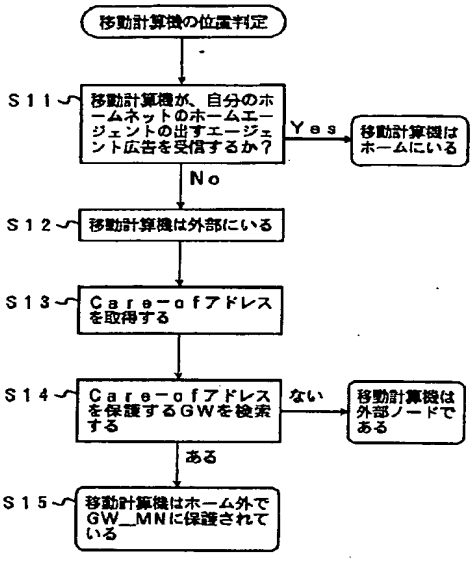
【図４１】同実施形態に係る移動計算機と通信相手の通信方法の一例を示す図

【図４２】移動計算機を含む通信システムの基本構成を説明するための他の図
【図４３】経路最適化を説明するための図
【符号の説明】
１，１ａ，１ｂ，１ｃ，１ｃ…ネットワーク
２，２－１，２－２…移動計算機
＊３…通信相手計算機
４，４ａ，４ｂ，４ｃ，４ｄ…パケット処理装置（ゲートウェイ）
５，５ａ，５ｂ，５ｃ，５ｄ…ホームエージェント
６…インターネット
＊２３…固定ノード

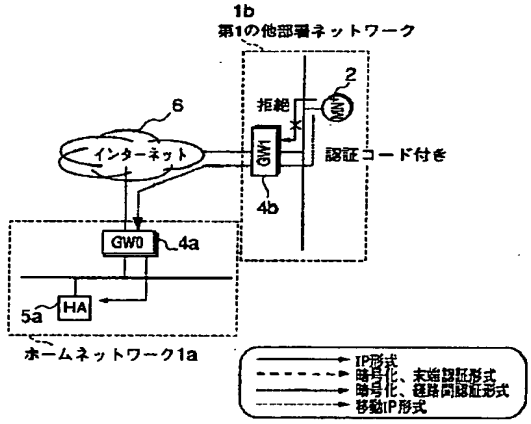
【図１】



【図３】



【図４】



【図５】

IP ヘッダ	KEY	AH	ESP	内部 IP ヘッダ	data（登録要求）

IPヘッダ（KEY）
送信元＝MNのケア・オブ・アドレス
宛　先＝GW0のグローバル・アドレス

内部IPヘッダ（登録要求）
送信元＝MNのプライベート・アドレス
宛　先＝HAのプライベート・アドレス

【図６】

IP ヘッダ	ICMP（通過拒否メッセージ）

IPヘッダ（KEY）
送信元＝GW1のグローバル・アドレス
宛　先＝MNのケア・オブ・アドレス

【図７】

IP ヘッダ	data（登録要求）

送信元＝MNのケア・オブ・アドレス
宛　先＝GW1のグローバル・アドレス

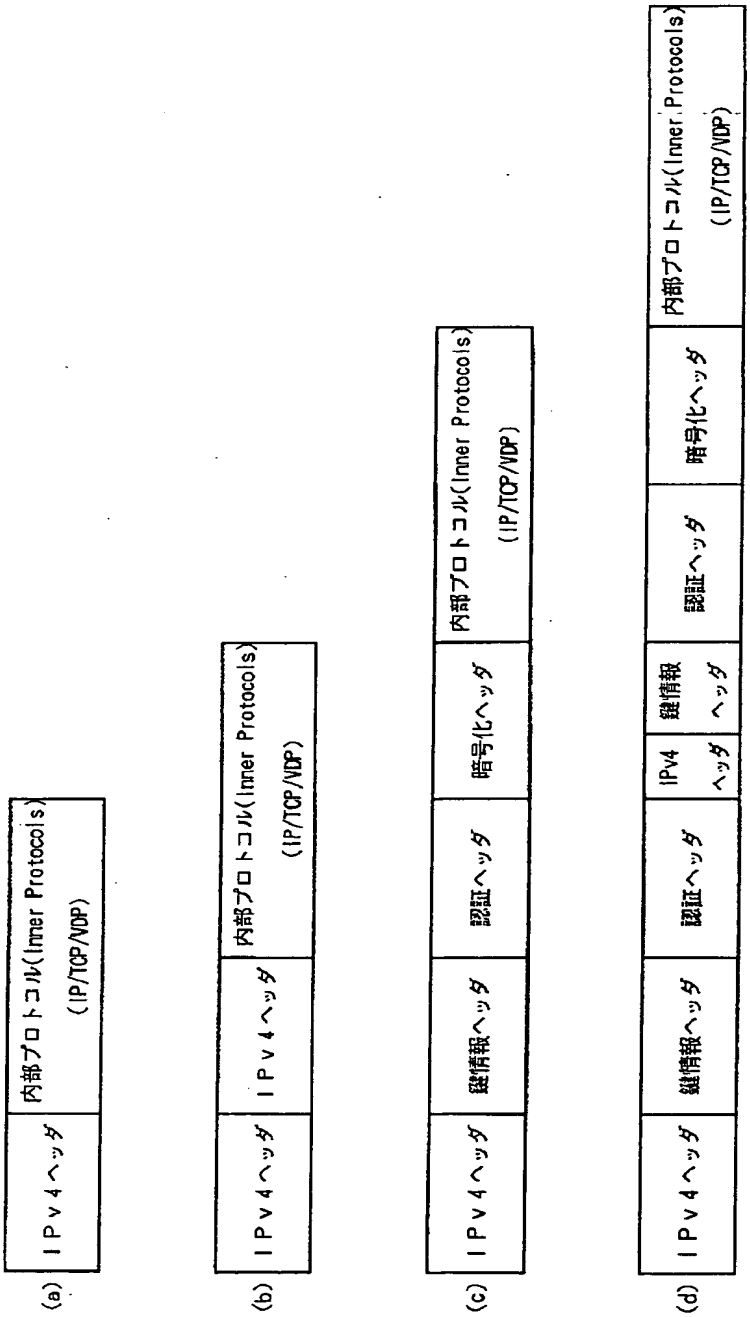
【図１０】

IP ヘッダ	KEY	AH	ESP	内部 IP ヘッダ	data（登録応答）

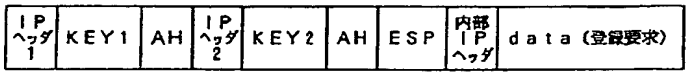
IPヘッダ
送信元＝GW0のグローバル・アドレス
宛　先＝MNのケア・オブ・アドレス

内部IPヘッダ（登録応答）
送信元＝HAのプライベート・アドレス
宛　先＝MNのプライベート・アドレス

【図２】


(a)
ＩＰｖ４ヘッダ
内部プロトコル(Inner Protocols)
(IP/TCP/VDP)
(b)
ＩＰｖ４ヘッダ
ＩＰｖ４ヘッダ
内部プロトコル(Inner Protocols)
(IP/TCP/VDP)
(c)
ＩＰｖ４ヘッダ
鍵情報ヘッダ
認証ヘッダ
暗号化ヘッダ
内部プロトコル(Inner Protocols)
(IP/TCP/VDP)
(d)
ＩＰｖ４ヘッダ
鍵情報ヘッダ
認証ヘッダ
IPv4ヘッダ
鍵情報ヘッダ
認証ヘッダ
暗号化ヘッダ
内部プロトコル(Inner Protocols)
(IP/TCP/VDP)
(経路間認証情報)
(末端間認証／暗号化情報)

【図８】

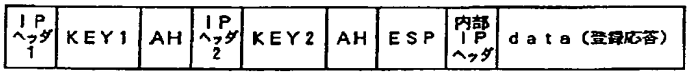


IPヘッダ1
送信元＝MNのケア・オブ・アドレス
宛　先＝GW1のグローバル・アドレス

IPヘッダ2
送信元＝MNのケア・オブ・アドレス
宛　先＝GW0のグローバル・アドレス

内部IPヘッダ（登録要求）
送信元＝MNのプライベート・アドレス
宛　先＝HAのプライベート・アドレス

【図９】

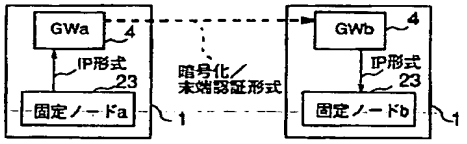


IPヘッダ1
送信元＝GW0のグローバル・アドレス
宛　先＝GW1のグローバル・アドレス

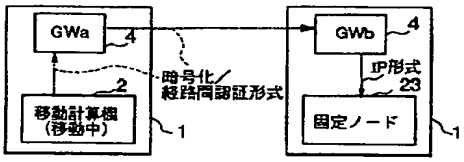
IPヘッダ
送信元＝GW0のグローバル・アドレス
宛　先＝MNのケア・オブ・アドレス

内部IPヘッダ（登録応答）
送信元＝HAのプライベート・アドレス
宛　先＝MNのプライベート・アドレス

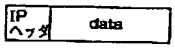
【図１１】



【図１２】

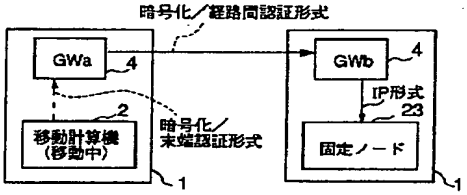


【図２４】

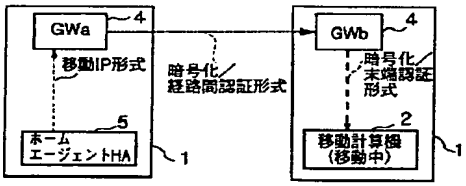


IPヘッダ(TCP/IP)
送信元＝MNのアドレス
宛先＝CHのアドレス

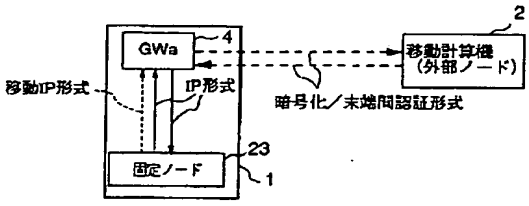
【図１３】



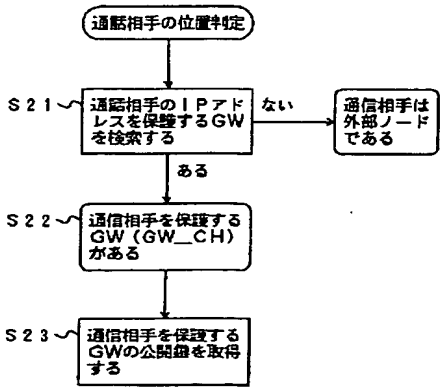
【図１４】



【図１５】



【図１６】



【図１７】

通信相手計算機CHの位置 ＼ 移動計算機MNの位置	GW保護域内	GW保護域外
GW保護域内	[1] GWを介したＩＰ CHアドレス：プライベート MNアドレス：プライベート	[3] 通常のＩＰ CHアドレス：グローバル MNアドレス：プライベート →プロキシーGWでグローバルに変換
GW保護域外	[2] GW*を介したＩＰ CHアドレス：プライベート MNアドレス：プライベート	[4] 通常のＩＰ CHアドレス：グローバル MNアドレス：プライベート MNはケアオブアドレスで普通にＩＰ通信（もしくはホームのプロキシーを経由したＩＰ．ホームまではＶＰＮ．）

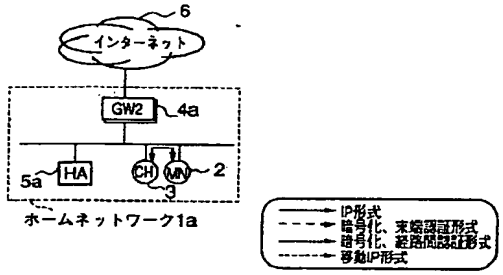
＊：MN付属のGW機能が動作するケース

【図１８】

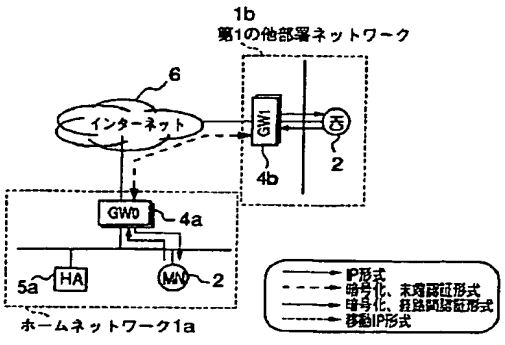
通信相手計算機CHの位置 ＼ 移動計算機MNの位置	NMのホームネット	他部署１
ホームネット	(1)	(2)
他部署1	(3)*	(4)*
他部署2		(5)*
外部	(6)*	(7)*

＊：MN付属のGW機能が動作するケース

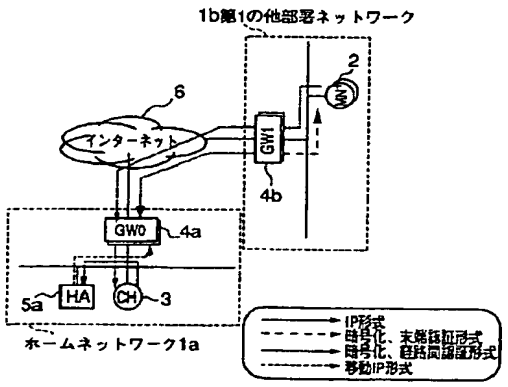
【図１９】



【図２０】



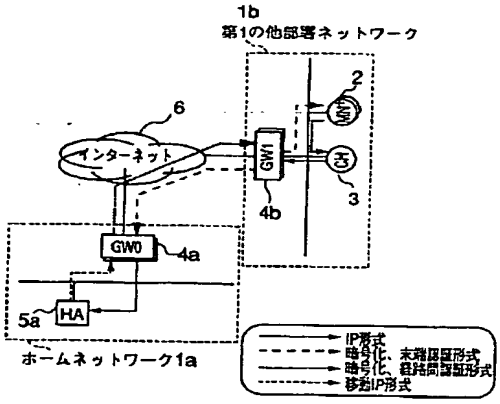
【図２１】



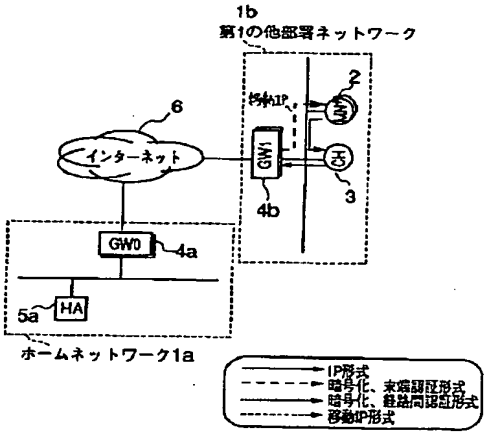
【図２２】

IPヘッダ1
　送信元＝MNのケア・オブ・アドレス
　宛先＝GW1(GW_MN)のグローバル・アドレス
IPヘッダ2
　送信元＝MNのケア・オブ・アドレス
　宛先＝GW0(GW_CH)のグローバル・アドレス
内部IPヘッダ（登録要求）
　送信元＝MNのプライベート・アドレス
　宛先＝CHのプライベート・アドレス

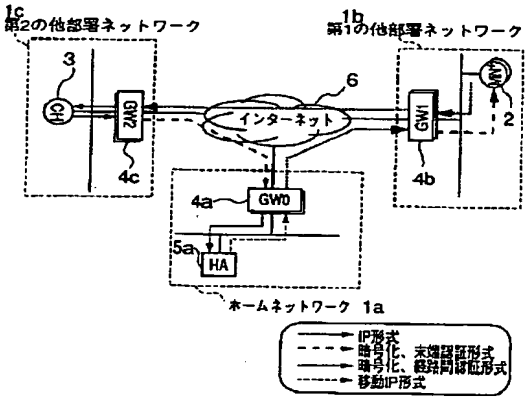
【図２３】



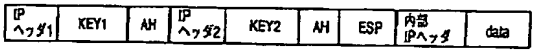
【図２５】



【図２６】

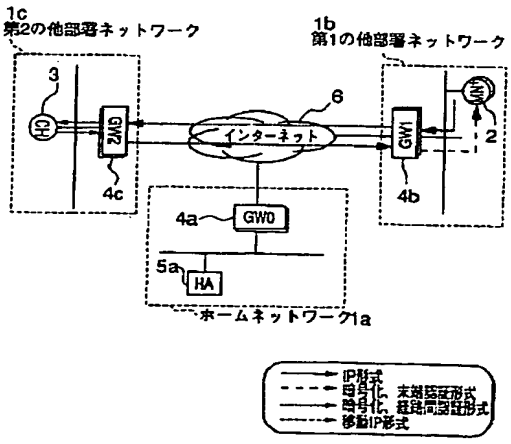


【図２７】

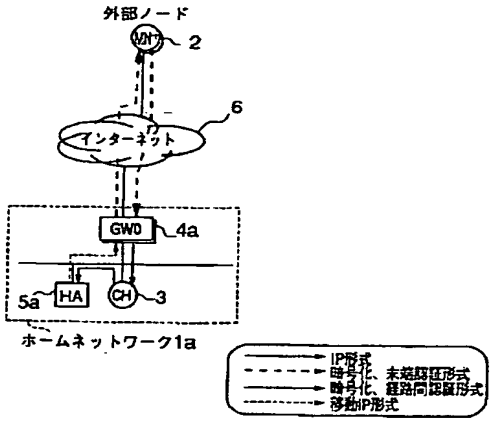


IPヘッダ1
　送信元＝MNのケア・オブ・アドレス
　宛先＝GW1(GW_MN)のグローバル・アドレス
IPヘッダ2
　送信元＝MNのケア・オブ・アドレス
　宛先＝GW2(GW_CH)のグローバル・アドレス
内部IPヘッダ（登録要求）
　送信元＝MNのプライベート・アドレス
　宛先＝CHのプライベート・アドレス

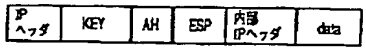
【図２８】



【図２９】



【図３０】

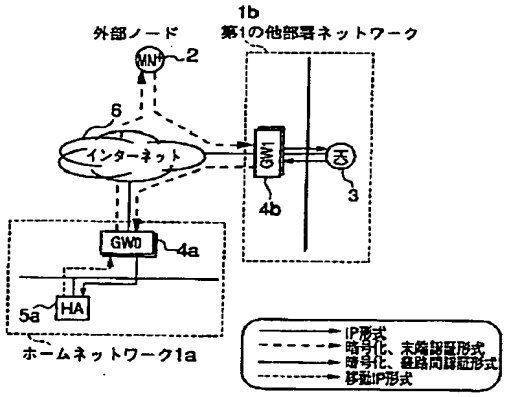


IPヘッダ1
　送信元＝MNのケア・オブ・アドレス(グローバル・アドレス)
　宛先＝GW0(GW_CH)のグローバル・アドレス
内部IPヘッダ
　送信元＝MNのプライベート・アドレス
　宛先＝CHのプライベート・アドレス

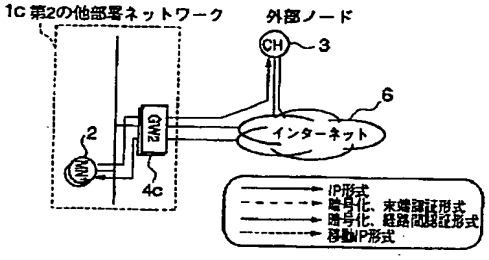
【図３２】

IPヘッダ1
　送信元＝MNのケア・オブ・アドレス(グローバル・アドレス)
　宛先＝GW1(GW_CH)のグローバル・アドレス
内部IPヘッダ
　送信元＝MNのプライベート・アドレス
　宛先＝CHのプライベート・アドレス

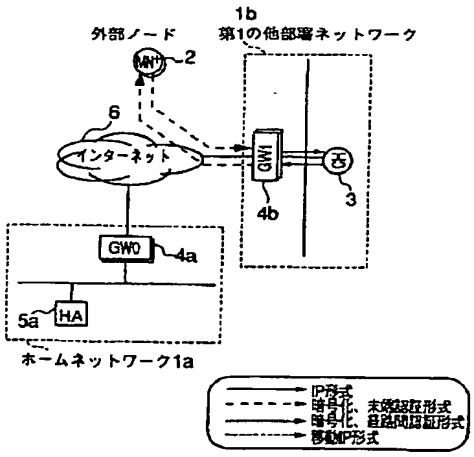
【図３１】



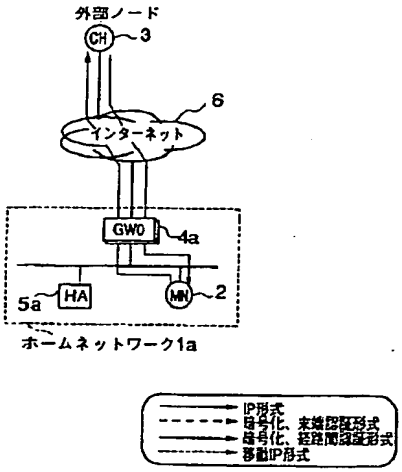
【図３６】



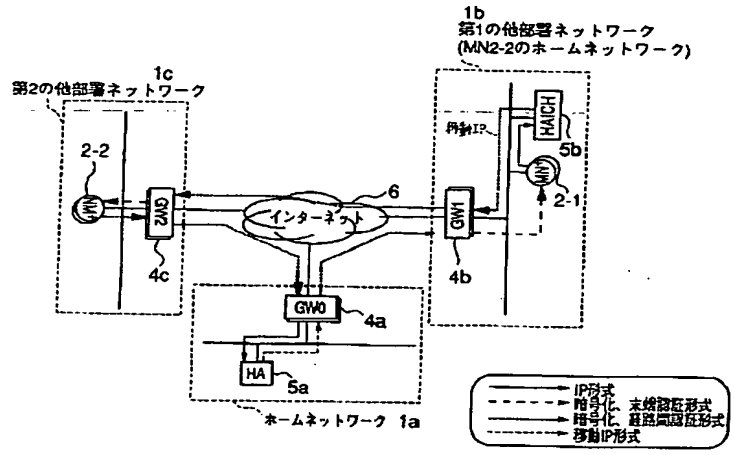
【図３３】



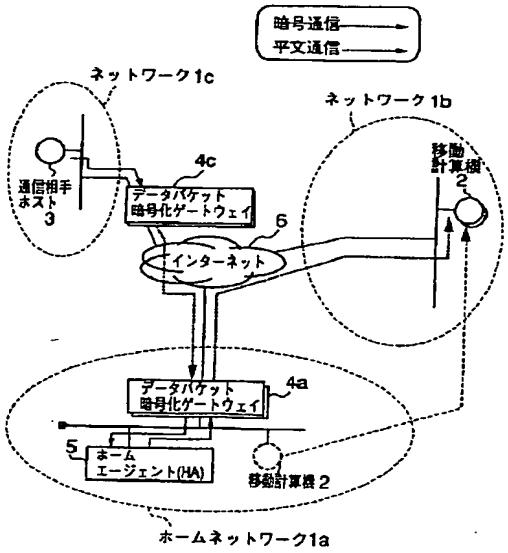
【図３４】



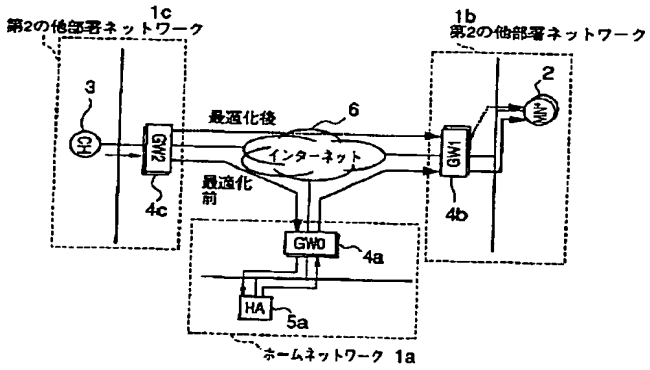
【図４０】



【図４２】



【図４３】



フロントページの続き

(72)発明者　津田　悦幸
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　新保　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　岡本　利夫
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内